Human Visual Based Perception of Steganographic Images

Blair Fyffe*, Yunjia Wang, Ishbel Duncan

School of Computer Science, University of St Andrews, St Andrews, Scotland

**now at Google Dublin.*

School of Computer Science, University of St-Andrews, North Haugh, St-Andrews, KY169SX, Scotland, Email: Ishbel.duncan@st-andrews.ac.uk

In 2014 it was estimated that 1.8 billion images were uploaded daily to the Internet, and in 2018 it is estimated that 3.2 billion images are shared daily. Some of these uploaded images may contain hidden information that can potentially be malicious (e.g. an image that contains hidden information regarding terrorism recruitment) or may cause serious damage (e.g. an employee wishing to hide sensitive company details in an image file and exporting the image to 3rd parties). This research studied the most effective methods in manipulating images to hide information (Data Loss).

Significant work has been done on computational algorithmic detection. Yet the desired output from this work was to find the point at which a human can no longer visually establish the difference between an original image and a manipulated image. This research examines the extent of use for file formats, bit depth alterations, least significant bits, message and audio concealment and watermark and filtering techniques for image steganography. The findings of this study indicated that audio insertion and picture insertion into cover image files are the strongest in deceiving the human eye. These results have been categorised for human visual perception in image based steganography.

Keywords: steganography, data loss prevention, human perception, image manipulation

Introduction

Data Loss Prevention is very topical due to the ever increasing number of cyber-attacks and data leakage incidents. Data Loss Prevention (better known as DLP) refers to the methods that identify, monitor, and protect data at rest, in motion, and in use, through extensive content analysis [1]. It is estimated that 90% of large organisations are targeted on an annual basis for data breaches and lose, on average, $3.15 million at a cost of $141 per data record [2, 3, 4, 5]. McAfee report 43% of all data loss is due to internal actors where an employee or someone with access to the computer systems maliciously exports sensitive data to external entities [6]. One of the ways in which this is conducted is by hiding information in media files to avoid detection.

However, the practice of concealing secret information is no recent discovery. This practice dates back over 2000 years and has been used in personal, political and especially military messages at times of war [7]. As early as 486 BC, the Greeks received warning of Xerxes' plans of attack from messages secreted beneath the wax of a clay tablet by dotting successive letters with secret ink [8]. Hundreds of years later, Mary Queen of Scots would utilise substitution ciphers to secretly communicate with her supporters while being held prisoner by Queen Elizabeth 1st of England.

The word 'Steganography' was derived by the two Greek words 'Steganós' (covered), and 'Graptos' (writing) which constitute a literal translation of 'cover writing' [9]. While classical cryptography (encryption) is about concealing the content of a message by 'scrambling' it where 3rd parties know communication has taken place [10], steganography is about concealing the very existence of the message altogether [8]. Luo *et al* defines Steganography as a technique for hiding information [11]. This definition, although vague, has been extended to define steganography as the art and science of communication, where the very existence of that communication is hidden [12]. To illustrate a representation of steganography in today's technological environment, it is an information security tool that stores secret information in a media file where only the

sender and receiver can discover the private data [13]. Steganography can ostensibly be mitigated by DLP, yet what techniques exist in DLP to prohibit its operations?

Data Loss Prevention Techniques

The best practices for Data Loss Prevention against steganographic practices are divided into two areas of research: data-at-rest and data-in-motion. Both areas cover the current 'industry standard' for data loss prevention.

Data-At-Rest

Data-at-rest refers to the data stored at an endpoint (such as a computer or mobile device) [14], where steganography predominantly involves the manipulation of static multimedia files by the user [15]. When a system is infiltrated, these users can either be internal (authorised user) or external (unauthorised user) and leak sensitive/confidential data. A common way in which this data is leaked is to embed the sensitive data into cover images (the image a user sees upon opening a file) or other forms of multimedia. Preventative measures, for data-at-rest steganography, often include the use of endpoint encryption or authentication such as by passwords, to prevent unauthorised parties, and restrict access to a subset of authorised users, or with potential steganographic tools that can be used to hide data within images [16]. Furthermore, the system could include physical media control to prevent the copying of sensitive data to unauthorised media to further prevent steganography and enhance DLP. This would leave the malicious user little choice but to transfer the sensitive data over the systems network to an external source, which then requires an application of data-in-motion security.

Data-In-Motion

This relates to any information that is transferred between endpoints over a network [14]. Data-in-motion steganography can often involve modifications to network protocols and deliberate deception to conceal the transfer of sensitive information [15]. This can be prevented by the use of network monitoring with packet sniffers, such as Wireshark, and firewalls and Intrusion Detection Systems to log and monitor network traffic and detect and investigate unauthorised sensitive data transfers [16]. In addition, secure email, secure API's and encrypted physical media ensure that data exchanges are only made with authorised 3rd parties and any unauthorised attempts would be flagged and reported.

Why Human Perception?

Data Loss Prevention, especially in industry today, relies heavily on the success of automated steganography detection algorithms that operate during the 'data in motion' phase combined with the strength of physical security in 'data-at-rest'. However, most steganographic techniques, for content based file formats, randomly place a hidden message in a cover image which is visually obvious to the human eye, but very difficult for even the most sophisticated algorithms to detect [17]. This leads to the question of why there is a significant lack of research in human visual detection of steganography. A DLP algorithm may detect an image, yet can a human visually detect inconsistencies in an image where algorithms cannot? If yes, then to what extent? This work conducted tests on this very subject.

Aims and Objectives

The aims and objectives of this research were as follows:

(1) To manipulate images using the following steganographic/conversion techniques: File Format; Bit Depth; LSB Images; LSB Text; Audio Input; and Watermarking & Filtering.
(2) To produce a table characterising the human deceptive value/effectiveness of steganographic methods.
(3) To establish the visible point of the 'strongest steganographic image' where an image can be modified until it can be spotted by the human eye.

To ensure valid comparative data, the experiment was conducted on a single machine to ensure there were no changes in resolution, brightness and screen quality for each participant.

Research Scope

This research produced 17 converted/manipulated images and compared them to the originals to evaluate the extent of human perception of steganographic images. The research built on research from previous academics that touched on the human perception aspects of steganography [18], while utilising the steganographic techniques to convert and manipulate the images necessary for the study [10] [19] [20]. Although the research incorporated some psychological aspects of research which can be used within the field of psychology, this research was purely aimed at, and operated within, the confines of the Computer Science security field. The research limited its scope to those

above the age of 18 and included both Computer Science and non-Computer Science participants of all age ranges and sexes.

Paper Structure

Following this 'Introduction' section, the 'Literature Review', will discuss both computational aspects as well as visual research, in order to gain a comprehensive understanding of work already done in steganography. The 'Methodology' will then convey the techniques and processes used to manipulate images and complete the conditions of the experiment and the objectives of the work. This is followed by the 'Results' section, where the outcome of the experiment is conveyed alongside a relevant critical 'Discussion' regarding the impact of the results on the field of study. The paper is then terminated with relevant references and how the work done in this area may contribute to human perception based steganography in the future.

Literature Review

This section critically analyses and reviews the multitude of work done for computational steganographic algorithms and the minimal work done for human visual based perception against images subjected to steganographic techniques.

Computational Steganography

Computational steganography, gained traction back in the early 1990's with the introduction of how algorithms could be utilised for steganography, giving birth to the Least Significant Bit (LSB) algorithm [19]. This introduced cover image steganography where using this LSB algorithm, text could be secretly embedded into a cover image. Cover image steganography has been the centre of debate regarding potential communication between terror activists, such as the attacks on the World Trade Centre in 2001 [21][22]. Current estimates of the number of images online vary between 675 billion and 1.2 trillion, making manual human checking for all steganographic images impossible [4][5][22]. This is why analysis algorithms are a necessity, in correlation with human visual detection, for Data Loss Prevention. Analysis may find patterns, such as keyword lists and hashing and report a concern for determination by human subjects [23].

Research then expanded to placing watermarks in images where the creator of the image could retain full copyright of their digital media [20]. Although this research did introduce algorithms for watermarking, the aim of this work was to show 'copyright

evidence' on the image itself, not to conceal the contents of the watermark. This research did, however, lead to the notion of hiding watermarks and their content for steganographic purposes. This was suggested in Johnson and Jajodia's paper [*10].* This landmark paper introduced the concepts of: concealing data in images; LSB; and masking and filtering. *Cox et al* portrayed how these concepts could be utilised to successfully conceal hidden data, and how masking and filtering could be used to hide the watermark content of images [20]. However, this paper only provided an overview of these procedures and lacked critical detail regarding the low level processes of these steganographic techniques and how they actually worked. Since then, extensive research has branched out to cover many aspects of computational algorithms for steganography.

Steganography Techniques

In recent decades, steganography has seen significant computational developments, in comparison to its previous use throughout history [10] [11] [24]. Yet why is steganography needed? Table 1 below compares the effectiveness of information hiding techniques for different motivational factors such as: confidentiality (ensuring communication remains between trusted parties only); integrity (no message tampering); and irremovability (named as 'unremovability' in [25], an inability to reverse engineer or decrypt steganography methods to reveal hidden information) [25].

	Confidentiality	Integrity	Unremovability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes / No	Yes / No	Yes

Table 1 - Comparing Message Hiding Techniques [25]

Table 1 highlights the value that steganography has for information hiding, confidentiality, integrity and irremovability, in comparison to alternatives such as encryption and digital signatures. Furthermore, steganography, when executed correctly, incorporates many techniques to conceal content without revealing its existence.

Least Significant Bit (LSB)

One technique to hide information is the Least Significant Bit algorithm, better known as LSB. This is a commonly utilised steganographic technique to embed information in a cover file. LSB can be used in the cover files of many forms of multi-media but it is used most frequently used for images. LSB manipulates specific bits of an image by changing the least significant values to avoid detection. An example of LSB's functionality for manipulating

the three primary colour values, red, green and blue (RGB) of an image can be seen below in Figure 1 [10].

The lower the LSB exchange, the harder it is to detect manipulation within the image. However, this adversely means that a smaller amount of information can be stored due to the limited number of least significant bits that can be manipulated. The higher the LSB exchange, the easier it is to detect manipulation in the image, yet a larger amount of data can be stored within the image due to the larger volume of bits.

The letter A is represented in binary by:

01000001

An example image is represented in binary as:

Red - *(00100111 11101001 11001000)*

Green - *(00100111 11001000 11101001)*

Blue - *(11001000 00100111 11101001)*

If the letter A were to be inserted into an image using LSB1:

Red - *(00100110 11101001 11001000)*

Green - *(00100110 11001000 11101000)*

Blue - *(11001000 00100111 11101001)*

This represents LSB1 as it only manipulates the 1st bit. LSB 2 would be represented as such:

If the letter A were to be inserted into an image using LSB2:

Red - *(00100101 11101000 11001000)*

Green - *(0010001 11001000 11101001)*

Blue - *(11001000 00100111 11101001)*

Figure 1 – The Least Significant Bit algorithm (from 10)

Watermarking and Filtering

A significant research area of image steganography is the use of digital watermarking. Images, especially those under copyright, may have a visual watermark placed on them that establishes ownership of the image. This technique can also be utilised to conceal information by 'blending' the watermark into the background of the cover image. Back in 2004, Cummins *et al* provided a popular, yet basic, interpretation of watermarking an image shown in Figure 2 below [26].

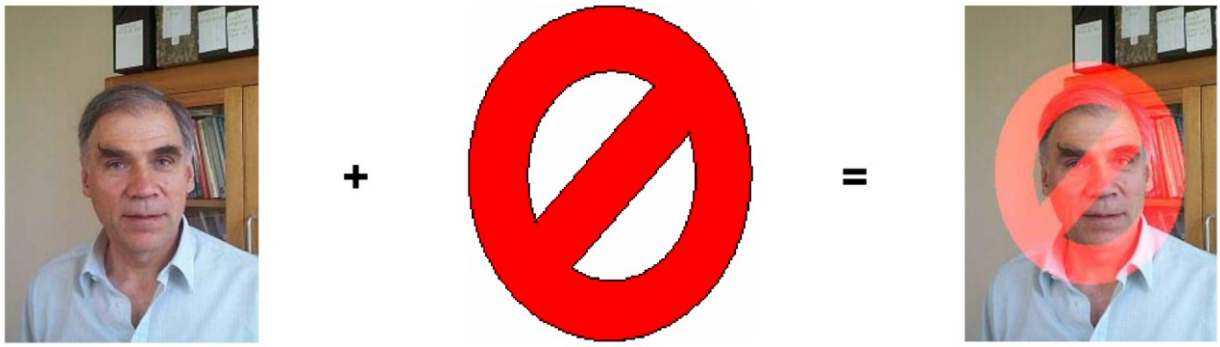


Figure 2 - Cummins et al providing a basic image watermarking technique [26]

Although Cummins *et al* did not provide the filtering process to hide the watermark, this has been manually done for the purpose of this study using a basic online filtering tool [27].

Figure 3 - Filtering Cummins et al's image for the sole purpose of watermark removal [26]

Figure 3 above shows how various filters can be utilised on an image to attempt to remove a watermark, yet this can often be at the cost of deviating from the integrity of the original image and its quality. As such, there is no tool that currently exists that recommends which filters to use on a certain image based on its resolution, contrast, colours, file format, bit depth etc. Thus images must be processed through filters manually.

Human Based Visual Perception

Steganography relies on the assumption that a human is not aware of the existence of any hidden data. This is one of the predominant reasons why steganography is argued to be just as, if not more, effective than cryptography. It is much easier to hide the existence of hidden data than to make its existence known e.g. where an attacker/investigator knows exactly what to look for i.e. a decryption key [28]. As human eyes are insufficient for detecting minimal changes in colour or positioning [29], steganography can be tailored specifically to exploit this inadequacy to the benefit of a malicious user, yet there is little research published in this field.

Limited research has touched on how humans see images that have been subjected to steganography [18]. Morkel et al discussed how humans perceive different file formats that have been subjected to the LSB algorithm, including JPEG, BMP and GIF. They declared JPEG and BMP to be the most effective in hiding information, yet other work states that PNG and BMP are more effective in concealing information [28][30]. Morkel *et al's* study [18] is only limited to file format perception and does not include the way in which humans perceive images that have been subjected to key steganographic techniques including: bit depth; LSB images; LSB text, audio insertion and watermarking & filtering etc. Moreover, this study dates back to 2005, only a year after the ISO/IEC declared the PNG file format as a standard [31]. This would justify why Morkey *et al's* study completely excluded PNG in their work.. This current study aims to update these findings and to add PNG to the research field for comparison by looking at how humans perceive different file formats of the same image.

Defining Scope

With steganographic techniques, such as the LSB algorithm and watermarking/filtering, data can be successfully concealed in images. Although steganography detection

algorithms are automated to detect hidden information in images, the most important area of steganography (and its core principles) is its ability to be imperceptible to the human eye [18]. The predominant amount of steganography detection research focuses purely on computational algorithms [32] [33] [34] [35] as opposed to the human visual detection elements. This presents an opportunity to explore new areas of research into human visual perception of steganography. This paper will therefore focus on this area with the aim to further develop this field by analysing how humans can visually detect various steganographic techniques.

Methodology

This section details the process of designing and building a steganographic test system for human trials along with the relevant technologies used for this work. Both successes and setbacks are documented along with relevant screenshots and steps so these processes can be replicated.

Design

The original image file formats to be used were JPEG, BMP and PNG. However, the BMP file format had to be changed to GIF as the Qualtrics survey software used for this study would not accept images of a BMP file format. The user interface was also important for participant interaction and to successfully engage a participant. Within the experiment, two images would be placed side by side for parallel cognitive processing [36]. This enables the participant to make a comparison of the two images. The grouping of two images for comparison will henceforth be defined in this work as an 'image set'.

Firstly, image formats were investigated and then in an experiment, two images with different formats or with one as an original image and the other as a cover image would be compared by volunteer participants.

Image Conversions

Original images (taken mainly from steganography based papers) were manipulated to generate output images that could be used in the study. All images conversions were used

from the resource list which included dual Hanns-G monitors and an XPC Shuttle tower on a Windows 10 operating system.

File Format Conversions

The first of the image conversions included a simple manipulation technique of importing an image into Microsoft Paint and converting the file format through the 'save as' function. The image sourced was 'Lena', which has been used in many previous steganography related papers and is a landmark steganographic image [15][37][38].

Initial attempts to convert the file format proved ineffective as changing the file format by manually re-naming the file extension in a directory did not convert the image. This was found by checking the files within a hex editor and discovering that the first four bytes, the signature of the file type, remained the same [39]. Analysis of the file size, where different file formats of the same image have different file sizes, demonstrated that the file size had remained the same.

The successful process of converting the file format with MS Paint can be seen in Figure 4 below. The Lena image was sourced online as a GIF [40] and converted to the PNG and JPEG file formats with MS Paint. These converted images were then verified with the use of an online hex editor to ensure a successful conversion had taken place (see Figure 5 below).

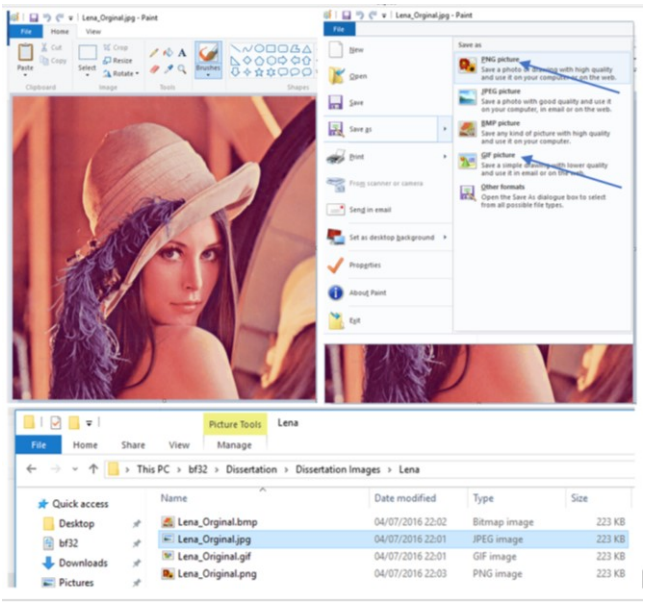


Figure 4 - Process of Converting the Lena File Format

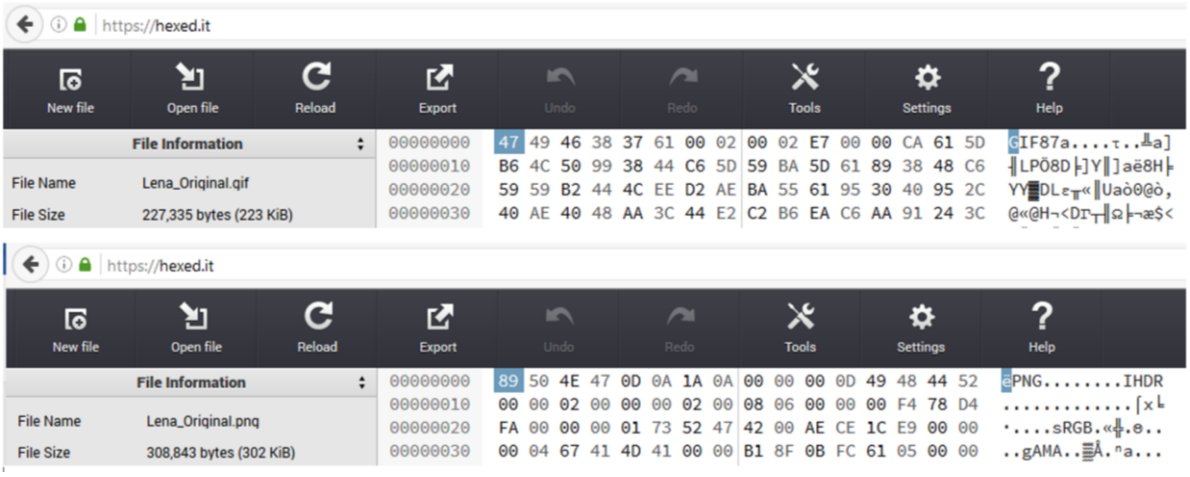


Figure 5 - Showing the Successful Conversion of GIF to PNG and JPEG

Bit Depth Conversions

The second image conversions were made to manipulate the original images (predominantly 24 bits by default) to a lower bit rate. The bit depth represents the amount of bits per pixel. The greater the bit rate, the higher the quality of the image due to the greater number of colours [10]. However, previous research claims that an 8 bit colour image is just as good as a full colour, 24 bit image [41].

To test this, the image selected for this was the Mona Lisa, arguably the world's most famous painting [42]. This can be beneficial to the study as a recognisable image is often easier to detect if there has been any manipulation, therefore truly testing the strength of the steganography technique.

The Mona Lisa was downloaded in a standard format of 24 bits online [43]. This 24 bit image represents 2^{24} colours resulting in a possible 16,777,216 colour variations by default [44]. The process of conversion can be seen below in Figure 6.

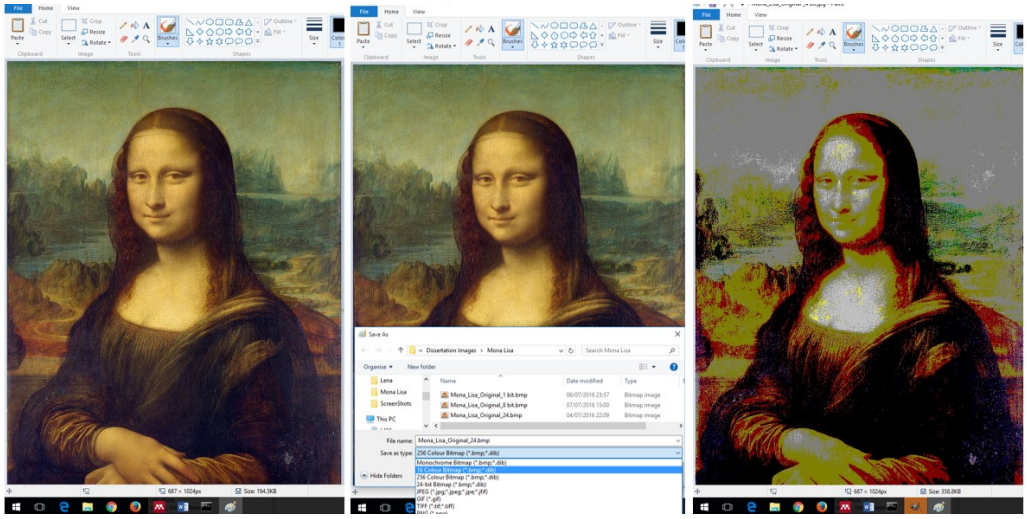


Figure 6 - Converting a 24 Bit Image (16,777,216 max colours) to a 4 Bit Image (16 max colours) with Microsoft Paint

The three conversions for the 8 bit, 4 bit and 1 bit versions of The Mona Lisa were initially attempted with GIMP 2.8, predominantly due to its ability to manually edit the maximum amount of colours the image could use. The image imported was a 24 bit image but GIMP only allowed a bit conversion down to an 8 bit image (maximum of 256 colours) and no higher, meaning a 12 or 16 bit image would not be possible for this section of the work [45]. Although the 8, 4 and 1 bit images could be created with GIMP, MS Paint is more widely established as an image conversion technique. Microsoft Paint was therefore used as a suitable alternative (as can be seen working with The Mona Lisa in Figure 6 above) to cover the full range of bit conversions of 8, 4 and 1 [46].

The Portable Network Graphics (PNG) was also used as a file format. As PNG is a lossless file format, this stores a better quality/closer matching copy of the image, whereas the Joint Photographic Experts Group (JPEG) is a lossy file format and focuses on smaller file sizes over image quality [10]. As image quality is one of the most important factors of the study, to ensure the most accurate research outcome based on human perception, a lossless file format (in this case, PNG) is used for various sections of the experimental tool, except for the audio cover files hidden within The Scream image sets (see page 15), where GIF is used (See 3.2.5), and JPEGs when used briefly for file format conversions.

LSB Image Input Conversions

These image conversions involved the use of the LSB algorithm, which was utilised to hide the Lena image into the Baboon image. This was done with the online tool, Incoherency, created by James Stanley [44]. Both Lena and the Baboon images selected for this section have been used in many previous steganography related papers [15][37][38]. The Baboon image was uploaded first as the cover image, followed by the Lena as the secret image. The amount of LSB places could be selected with a sliding bar as can be seen in Figure 7 below.

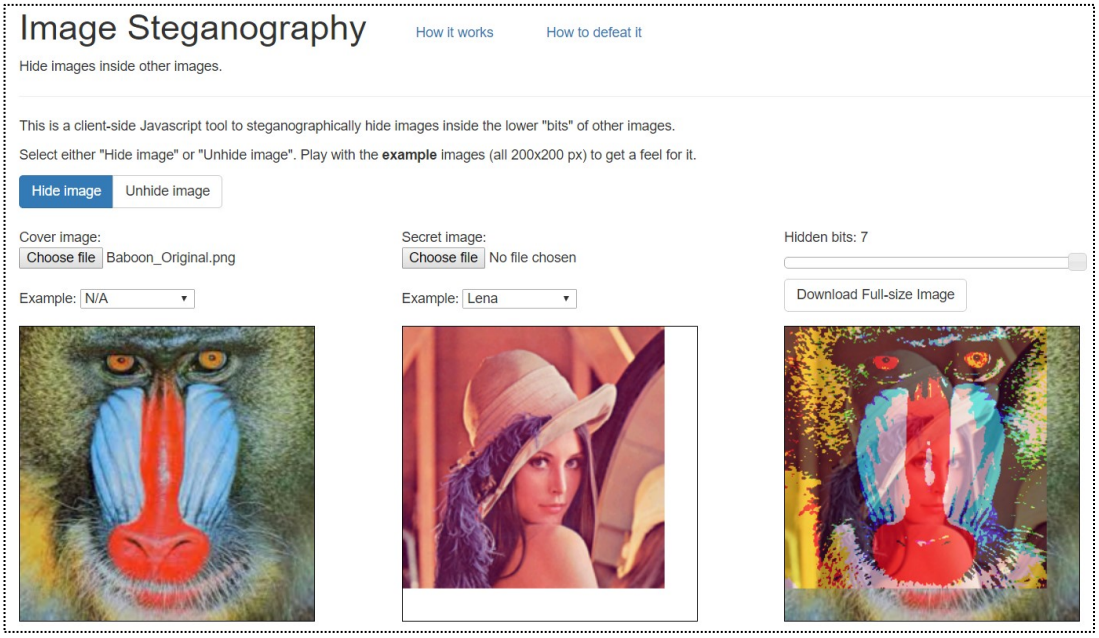


Figure 7 - Showing Lena Image being placed into the Baboon Cover Image with LSB 7

The output images utilised LSB1, LSB3, LSB5 and LSB7. Furthermore, the images uploaded and used for this section were also in the PNG file format, used for its lossless compression technique.

LSB Textual Input Conversions

After extensive research into textual steganographic tools, there was only one reliable option online, 'ManyTools – Steganography' [48], yet this only enabled the use of LSB1 due to a 250,000 character maximum as can be seen in Figure 8 below.

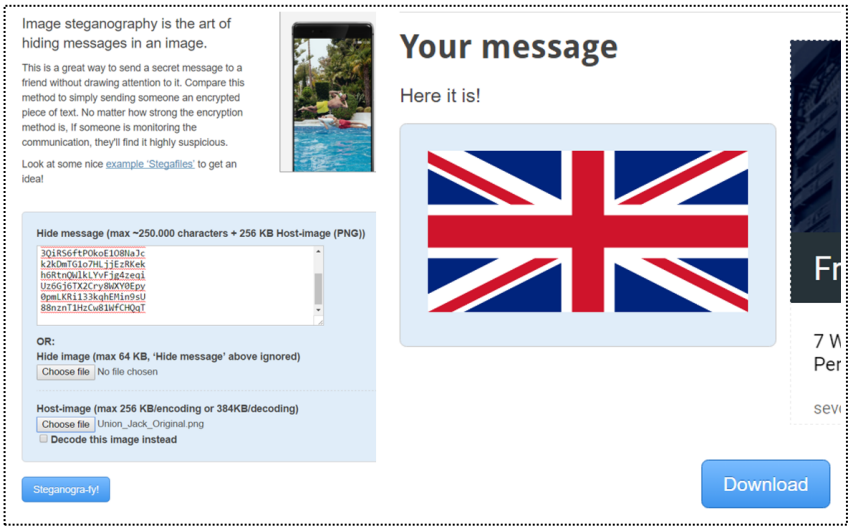


Figure 8 - Using LSB1 to Insert Text into Image

However, software named '*StegoUI*' was under development by a co-author and this provided the unique functionality to select various LSB values to hide text within an image [49]. This software allowed a range of LSB numbers from 1 to 8 [50]. The output file could also be converted to an alternate file format including JPEG and PNG. PNG was selected for the purpose of this study due to it's lossless compression technique [28][30], it's ability to store a better quality/closer matching copy of the image [10] and it's lack of coverage in previous human visual steganography studies.

Random strings were generated to populate the text to be hidden within the images. Manually this would take too long so a random string generator was used [51]. Utilising the LSB 8 manipulated image as an example, 50,000 words containing 20 characters each were generated, totalling 1,000,000 characters to hide within a Union Jack Image. This particular image was chosen due to its hard lines (the solid straight lines within an image), where any 'squints' or 'disfigurements' in the hard lines of the image would be easily detected by a participant of the experiment.

This text was then copied to a .txt file and saved for later use for *StegoUI*. The original 'Union_Jack.png' image was imported into the text hiding software. The previous text file, containing the 1 million characters, could now be imported into the Qualtrics software to be concealed within the Union Jack PNG image. The necessary output file format could be selected, along with the bit exchange in this case 8 bits, as shown below in Figure 9.

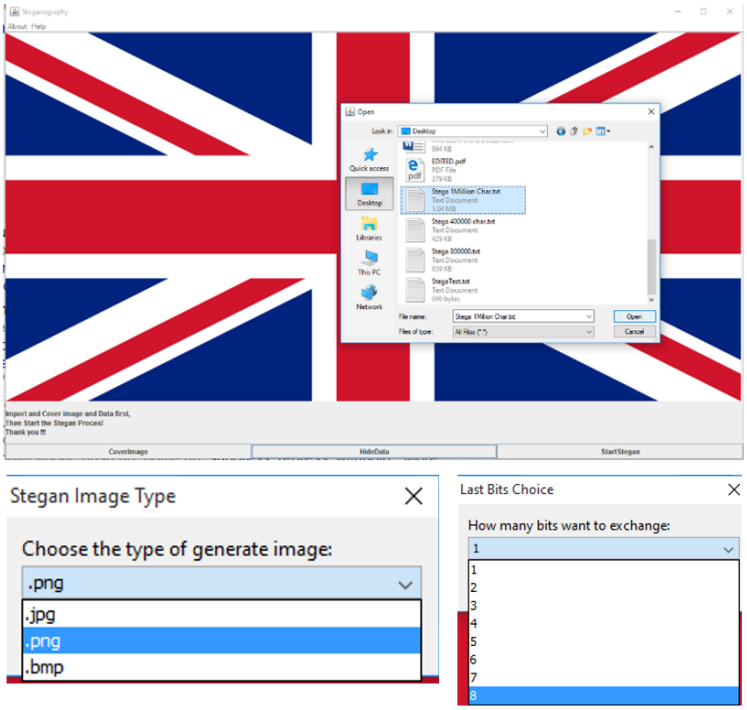


Figure 9 - Importing Text, Selecting Output Format and Bit Exchange for Union Jack

Processing this image, especially across an 8 bit exchange, took on average of between 8-10 hours to fully process due to the large volume of characters. Once this process successfully completes, the image is shown within the development environment and then output to the software's destination folder (see Figure 10 below).

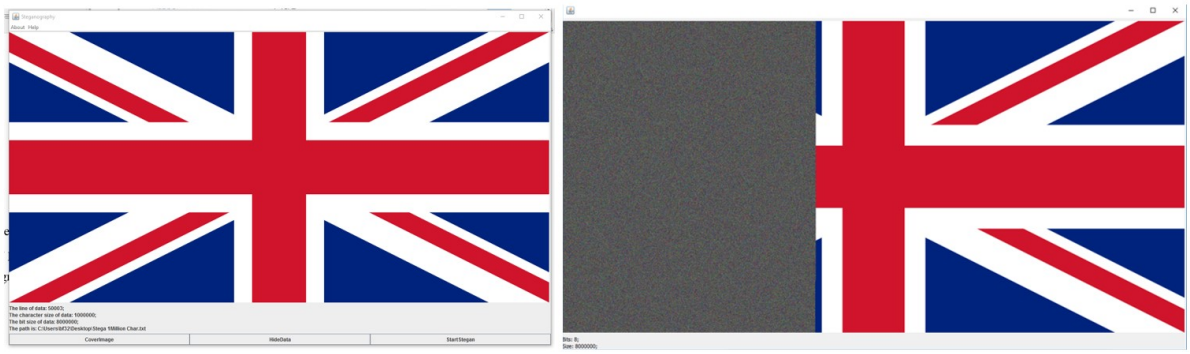


Figure 10 – Output from SteganUI of 1 Million Characters, Hidden in Union Jack with LSB8

The output files were then imported to Qualtrics along with all other selected instances of LSB 1, LSB 4, LSB 6 and LSB 8. If all LSB's were used (from 1-8) it would have

cluttered the survey with too many images of the Union Jack, as well as prove difficult for a user to notice any significant change between LSB increments of 1.

Audio Input Conversions

Audio files were then placed into image sets for the study. The Audio file entitled, 'bell-ringing-01.mp3' was an mp3 file with a 16 second duration, and a 672KB file size (0.672MB), sourced online, legally, for free [52]. The mp3 file format was chosen due to its status as the most popular file format for digital audio compression [53]. The bell audio file was placed into a GIF image file because of its lossless compression and also because PNG could not be used with this method. The image used was the 1893 version of 'The Scream' painting by Edvand Munch, obtained online as a JPEG [54] as shown in Figure 11, then converted to a GIF file format through MS Paint making the size of this GIF file 7.28MB without audio insertion.

Figure 11 - The Scream 1893

The audio file is placed within the image file, 'The_Scream_Original.GIF' to create a new file altogether, 'Scream_Bell.GIF' [55]. The manipulated output image file generated from this process is 7.94MB, 0.66MB larger than the original file, conveying that the audio file is successfully saved and concealed within The Scream image.

There were, however, limitations to this technique as the audio file bits are added to the image file instead of replacing the bits already there. This causes the file size to increase dramatically. This was evident on the first attempt of this section of work when using Beethoven's 9th symphony 1st movement, *"Allegro ma non troppo, un poco maestoso (D minor)"*. This caused the file size of the original Scream GIF image file to increase from 7.28MB to 42.9MB and conflicted with the 16MB file size limitation offered by Qualtrics. The bell was chosen as a suitable alternative due to its significantly smaller file size.

A second cover image of 'The Scream', for the next image set, was generated using a larger audio file, *"Richard Wagner – Ride of the Valkaryies"* with a size of 4.57MB and at a length of 5 minutes which is much longer than the ringing bell used previously. The Wagner audio file was obtained from the video streaming platform, YouTube [56], and converted with a 'YouTube to MP3 converter' [57].

The Windows command prompt was utilised once again and produced a slightly larger output file size of 11.8MB, which would be compatible with Qualtrics 16MB file size limit.

Simple cross multiplication to find the missing proportion can indicate the maximum audio time limit that can be used to 'hide' audio in The Scream input image using this technique, without exceeding the Qualtrics file size limit. This is calculated as: ***16MB = 11.8MB/Time = 6.8 mins = 6m 48s.***

Even if an audio file was sourced at the exact limit of 6 minutes and 48 seconds, there is a low probability of a user seeing much visual difference in an extra 4.2MB that has been 'copied' and not 'blended' together to make the output image.

Watermarking and Filtering Conversions

The image to be used for the final image sets is Leonardo Da Vinci's, *'The Last Supper'*. This depiction is argued to be one of the most analysed and recognisable paintings of all time [66], arguably easier for humans to notice any alterations based on their prior knowledge and memorisation of this painting. Watermarks can be applied to this image and concealed with filtering. The website 'Watermark.ws' was utilised to generate a watermarked image of 'The Last Supper' painting [67]. A simple caption was used with the

websites default text (calibri) and colour (white) placed over the front facing section of the table cloth in Da Vinci's painting (see Figure 12).

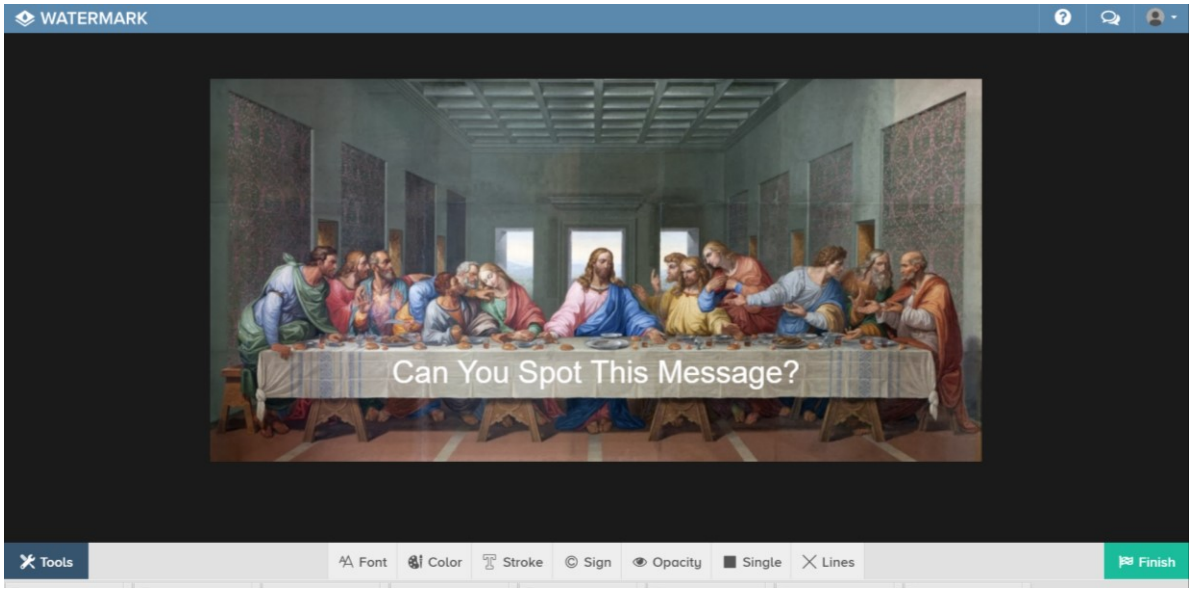


Figure 12 - Placing a Watermark Message in The Last Supper Painting

The output painting, along with the watermark, is then uploaded as a PNG to the free online filter editing software, Pic Monkey (see Figure 13) and processed through several filters (named 'effects' in Pic Monkey) to see how different filters can conceal the watermark [27].

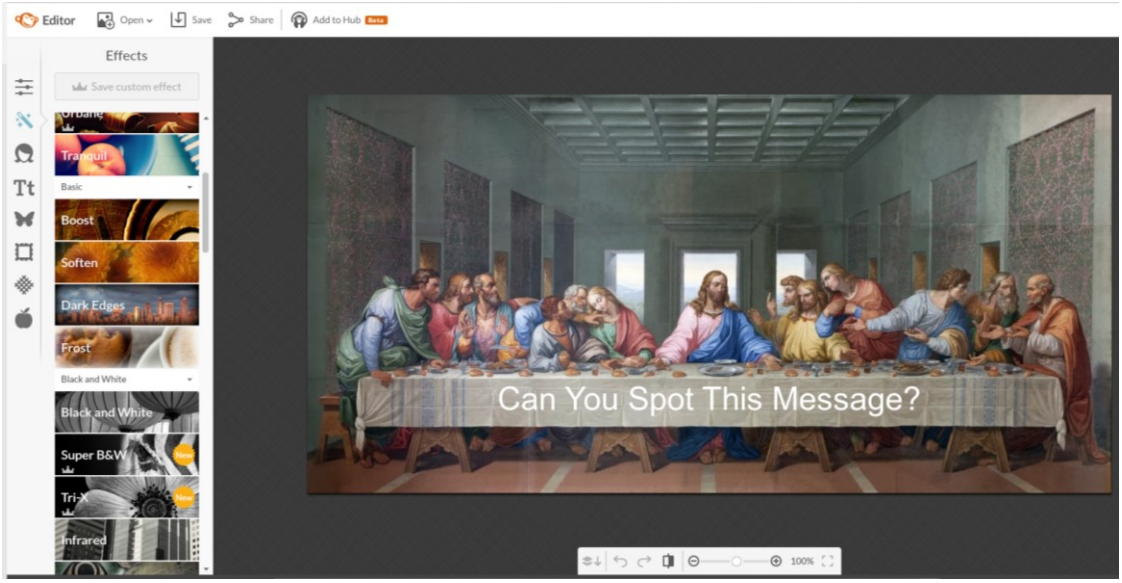


Figure 13 - The Last Supper Uploaded to the Image Filter Editor

For ‘The Last Supper’ painting, each of the 52 filters available were experimented with to conceal the watermark. These filters alter the colours available, the contrast and brightness and in some cases, the amount of pixels available. The filters chosen are the ones in which the watermark caption is best concealed visually, all while maintaining, as closely as possible, the visual integrity of the original image. Upon choosing a filter, there were variations and manual editing options to the defaults that could be made for more specific editing such as brightness, fade (contrast) and bloom (sharpness) which can be seen in Figure 14 below, yet the standard defaults of each filter were not sufficient to hide the caption without significant manipulation to the original image. All necessary edits made to the chosen filters can be found in the several figures within this section and this will be easier for replication in future work when hiding watermarks.

The initial watermark used white text as the default, yet this proved inadequate to successfully conceal the message with filtering without significant manipulation to the original integrity of the painting. This is evident in Figure 14 below.

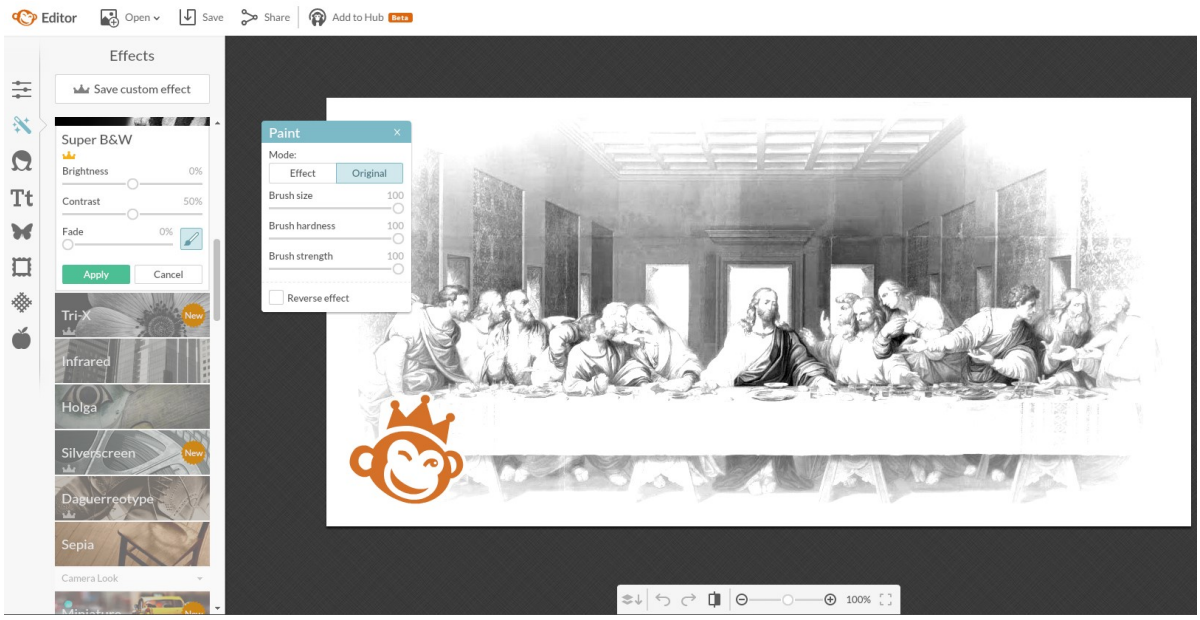


Figure 14 – Closest Filter to Effectively Conceal White Colour Font

The edits made above successfully conceals the watermark, yet deviates from the original integrity of ‘The Last Supper’ painting. The whole process was reset and another attempt was made to find a font colour (when watermarking) that matched closely to a section of the painting where it could be easily concealed (see Figure 15 below for the

new watermark). The font style and its size was still the same as the watermark caption used in the previous attempt, yet the colour was selected more carefully toward a dark grey to blend into the table cloth more effectively.

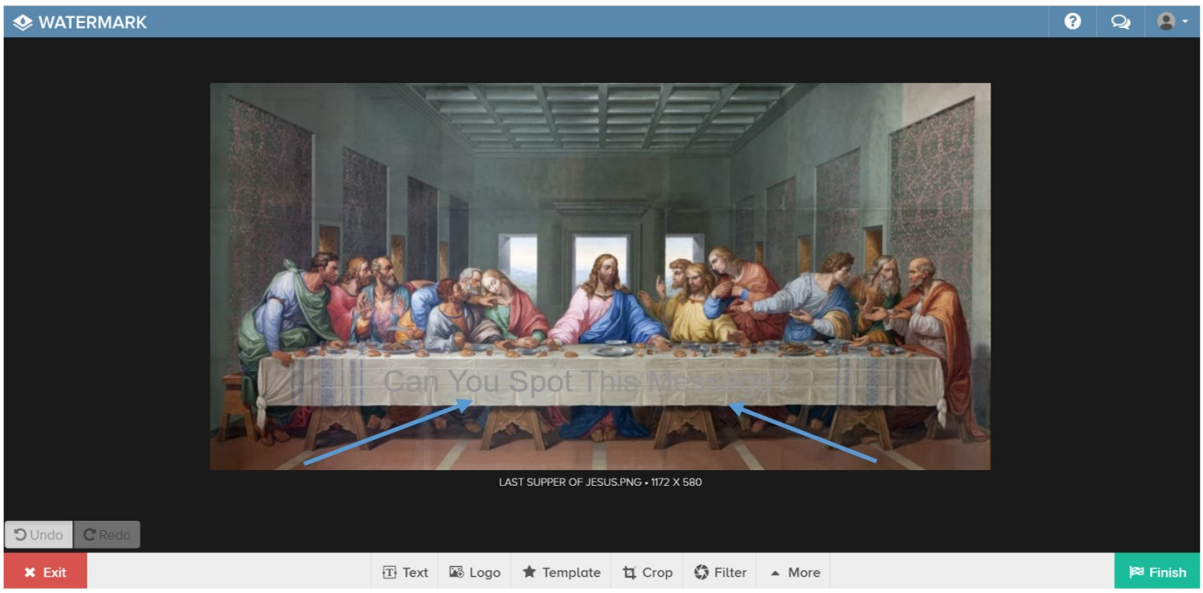


Figure 15 - Using Different Font Colour To Hide Caption More Effectively

The new watermarked image (without any filtering) is to be compared with the original 'Last Supper' painting in an image set in to analyse whether watermarking, with a carefully chosen font, is enough to hide a caption/watermark successfully without the use of a filter. However, as this is uncertain until the results of the experiment are published, the new watermarked image is still processed through the filtering software regardless, predominantly on the basis that the caption in Figure 15 above is obscured but not invisible.

The following filters were applied to the image:

1. ‘Soften’

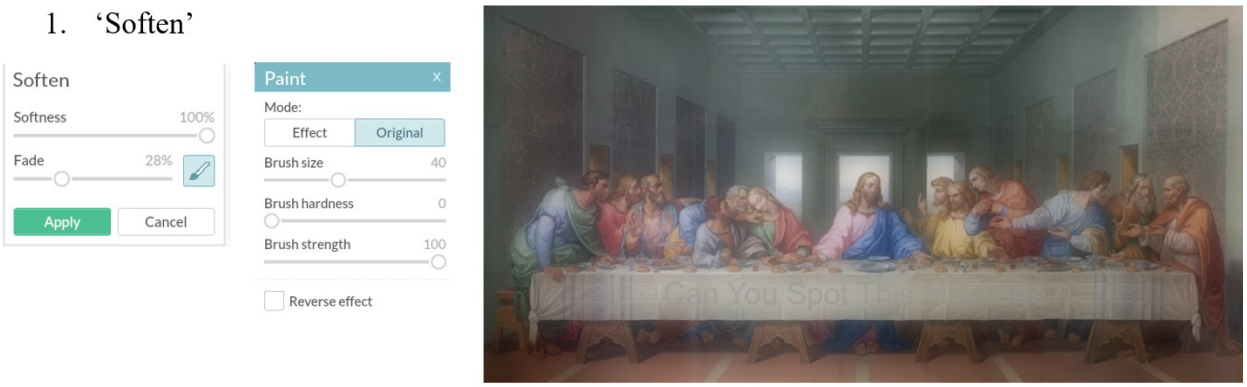


Figure 16 - Soften Filter Applied to Watermarked Image

2. ‘Cinemara’

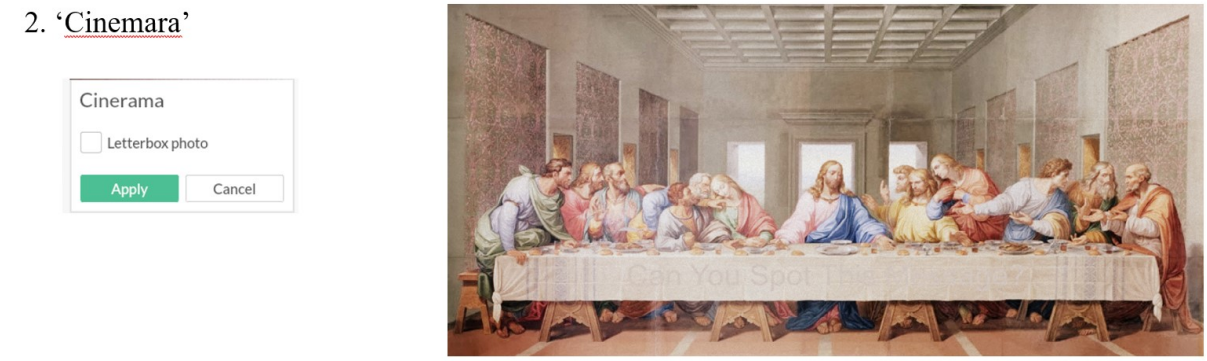


Figure 17 - Cinemara Filter Applied to Watermarked Image

3. ‘Bokeh Shapes’

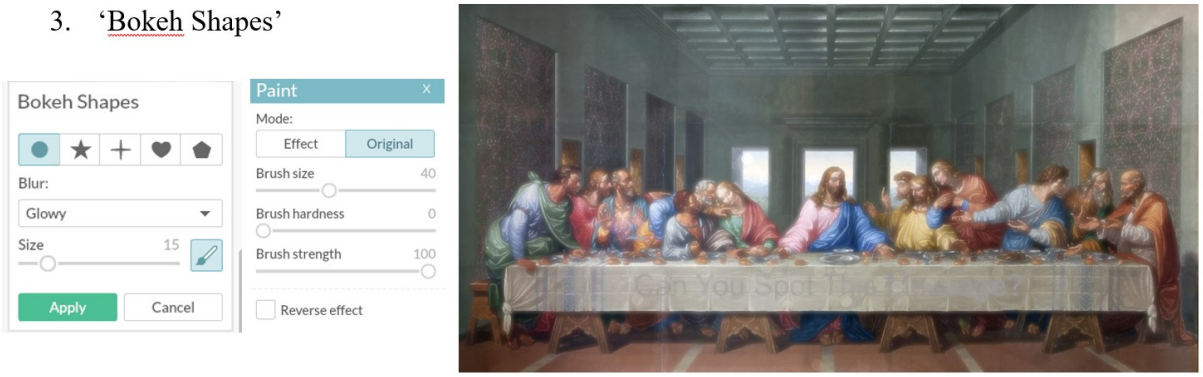


Figure 18 - Bokeh Filter Applied to Watermarked Image

For the experiment, if a watermark is placed within an image, these watermarks can often be hidden using filtering techniques, therefore the aim of the filter section of the experiment is for the participant of the study to select which filter they perceive to be the most similar to the original, making it easier to successfully hide watermarks within an image. The output manipulation images were saved as PNG files and uploaded to the Qualtrics project tool as the last image sets, as explained in the following section.

Image Uploads

All the images (both original and manipulated) required to be uploaded to the Qualtrics survey software. Each image was given a resolution breadth of 317 by default. This provided enough space to include the original and the manipulated images side by side for easier viewing for the participants of the study. See Figure 19 below for an example with 'The Mona Lisa'.

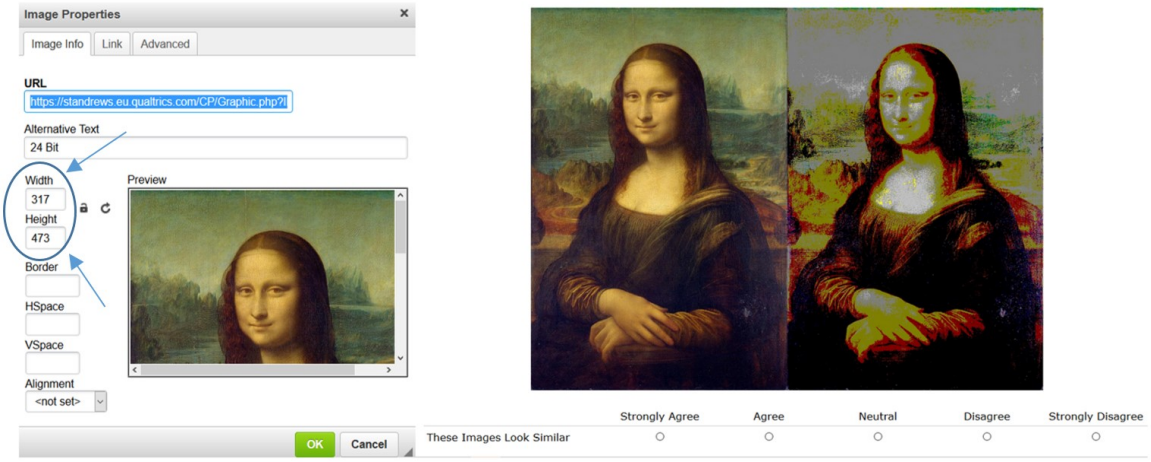


Figure 19 - Mona Lisa Upload to Qualtrics

The height varied depending on the stored file's height of an image. The height, however, was irrelevant compared to the width just as long as the original and the manipulated were displayed side by side. After all the original and manipulated images were uploaded to the platform and formatted along with all relevant information, the environment of the experiment could be designed.

Experiment

The participant of the study is asked to sit down and conduct the experiment from an Apple MacBook Pro 15 Inch with a retina display. The MacBook had been chosen predominantly due to its portability, enabling more participants, especially living out-with a lab environment, to conduct the study with the ease of bringing the experiment to them [58].

This model of MacBook Pro also has an Ambient Light Sensing (ALS) system that automatically adjusts the brightness of the display in proportion to the light available in the laptops location [59]. This feature will be turned off to ensure each participant involved in the study is presented the experimental display with the exact same screen brightness. No evidence was found to indicate whether the charging of a MacBook provides a greater brightness than without, therefore for portability, no charger will be used while the participant is involved with the study.

The following screen features are applied to the MacBook Pro:

- Brightness = 100%
- Ambient Light Sensing = Off
- Resolution = Default (2880 x 1880) and 220 Pixels Per Inch
- Display Profile = 'Display'

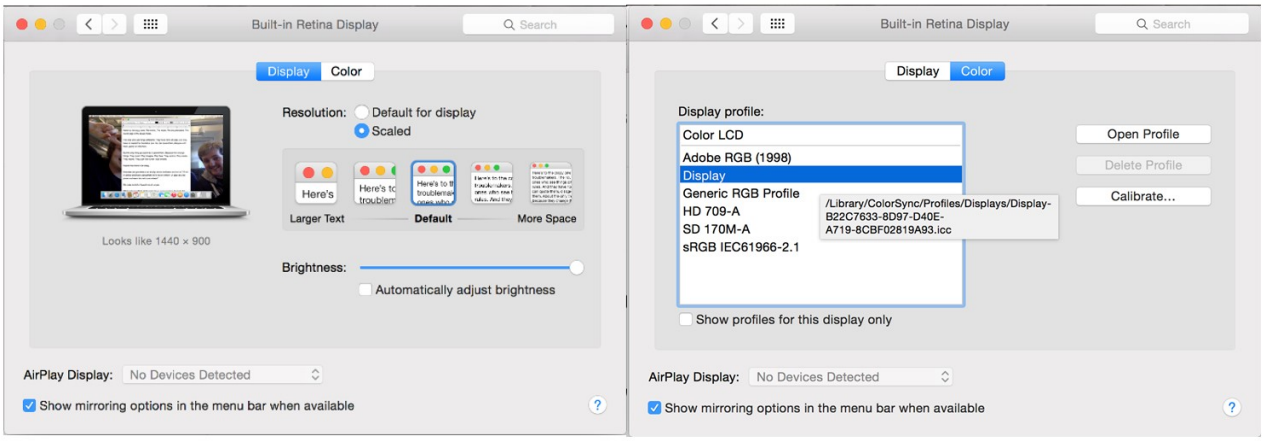


Figure 20 - Display Setting of MacBook Pro Used for Experiment

Informal alpha testing estimated the full study, including reading of the ethics and debriefing forms, to take somewhere between 10-12 minutes per participant. The participant is audio recorded during the experiment to hear their thought process and decision making spoken out loud for the benefit of the study. Furthermore, vocalising thought processes during the experimentation has been proven to be beneficial for research purposes to engage the participant more with the study [60].

For any one question, the user is shown an image set, two images side by side sequentially, where one image is the original and the other image is manipulated (either minor or majorly) yet the user is not told which is which. The participants are asked to judge the visual 'similarity' between the original and the manipulated images.

Key Information

(1) Below is the itinerary to the study:

(2) The participant is asked to read a hard copy of the participant information form to confirm they understand what will be required of them = ***2 Minutes***

   a. Before starting, the participant is asked to provide verbal confirmation that they have read the participant information sheet and agree to being verbally recorded during the process.

(3) The participant is then asked to open the Qualtrics survey = ***10 Seconds***

(4) The participant then reads the full ethics form = ***2 Minutes***

   a. Computationally agrees to all experiment conditions

(5) The survey starts and the participant is asked to, "Please take 10 Seconds minimum to analyse each question carefully" = ***3 Minutes and 30 Seconds***

   a. Asked to answer 17 Questions with 2 images per question (1 image set)

      i. 34 Images to analyse in total

      ii. Gives answers based on the statement "These Images Look Similar"

   b. The participant is verbally asked if they have seen the image set before

(6) Participant then submits their answers and reads debriefing form = ***2 Minutes***

(7) The study does not include anyone below the age of 18 for ethical purposes and the interviewer is present for the duration of the experiment with each participant while being audio recorded.

Scoring

Scores were allocated to each answer a participant gave for each image set. Scoring, on a descending scale from a maximum of 5 to a minimum of 1, was assigned to each question in the Qualtrics experimental tool in accordance with the use of a Likert scale. This scale was selected due to its popularity in attitude based experiments, its simplicity and versatility [61]. The scoring was assigned based on the similarity between two images, the closer the visual similarity, the higher the score (closer to 5) the manipulated image would receive. The wording of the statement was selected carefully to evaluate how respondent's definition of "These images look similar" influenced their decision process. The manipulated images with the highest scores are the most visually effective in concealing information. With this quantitative data, the point at which a human can no longer visually establish the difference between an original image and a manipulated

image can be sourced (see page 42 under '*The 'Strongest' Steganography Image'*). This would give an indication towards the extent of steganographic values for file formats, bit alterations, LSB message and audio concealment and watermark and filtering techniques. Furthermore, the result of this study, based on scoring, will output the best combination of all these techniques for different kinds of visual deception.

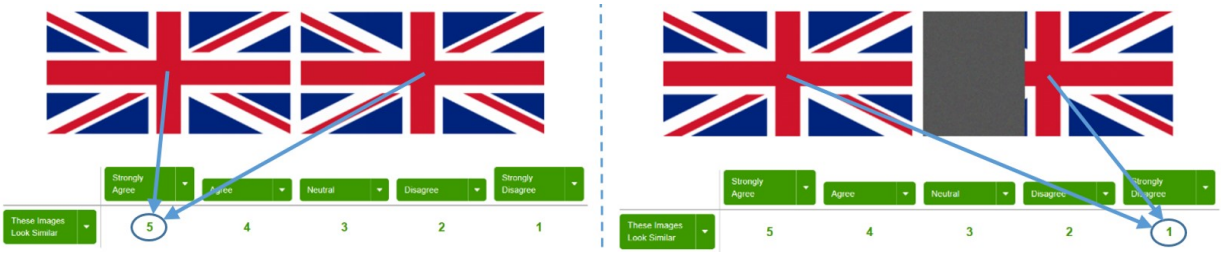


Figure 21 - Differences in Scoring Between Two Questions

The example in Figure 21 above conveys how this project's scoring was applied to the Qualtrics tool. This shows two Union Jack images (left of the blue line in Figure 21 above) where one is the original, and the other is the manipulated image the with 200 characters hidden within LSB 1. As both these images are visually identical, the manipulated image is therefore given a score of 5. The other two visually unidentical images (right of the blue line in Figure 21 above) conveys an original Union Jack, while the other image contains 1 million characters hidden in LSB 8, resulting in a score of 1 on the Likert scale. This example would indicate that LSB 1 in the first set of Union Jacks is a stronger use of steganography than LSB 8. The participants' scores for each image set are collected and calculated to find the mean score. The higher the mean score, the stronger the value of the steganographic/image conversion technique in deceiving the human eye.

Results

The central aim of this work was to manipulate images using steganographic techniques, categorise the results from strongest to weakest and to suggest the most efficient ways to hide different types of data in images with the 'strongest steganographic image'. This section will detail these results from each of the image sets and produce the findings to demonstrate steganographic strength.

Key Information - Participants

There were a total of 50 respondents over a seven day experimentation period. Each participant gave their full consent to the study and to being audio recorded during the experimentation process. Experiment length and average scores are rounded to the nearest value accordingly, with no decimal place, as can be seen in Table 2.

Participant Information	
Participant Characteristics	***Stats***
Average Experiment Length	5 Minutes
Males	25 Participants
Females	25 Participants
Average Age	30 Years
Computer Science Background	21 Participants
Non-Computer Science Background	29 Participants
Wears Glasses	18 Participants
'Sometimes' Wears Glasses	18 Participants
Wears No Glasses	14 Participants

Table 2 - Detailing the Variation of Participants Used for the Study

Overall Image Comparison Results

This section displays the overall results across the 50 participants involved in the experimentation process. Each section will have the dual images as thumbnails to remind the reader what images were being used for the tests. Relevant clips from audio recordings are presented using quotations to gain a deeper understanding into why participants selected the answer that they did. Lastly, each figure will contain a mean Gauge chart (at the top right hand side of each figure) to convey the similarity between the images. With the exception of file formats, each image set that has a higher mean score (closer to 5 and green) will be seen as a stronger steganographic technique. A lower mean score (closer to 1 and red) will be regarded as a weaker steganography technique with blue signalling a more central Likert scale score.

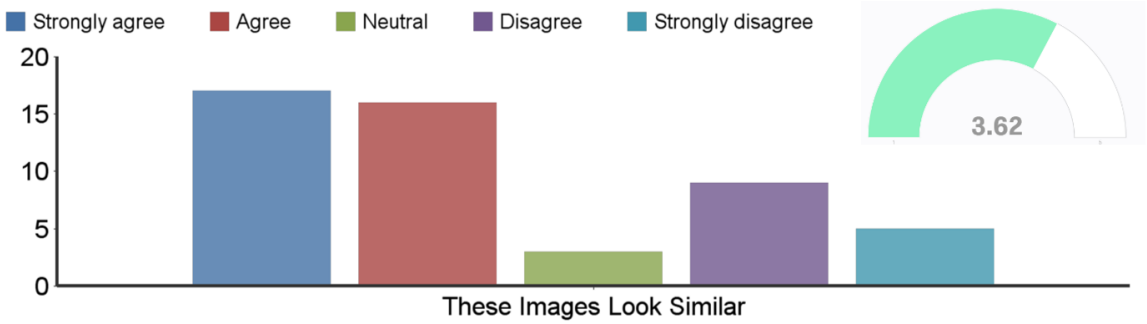
File Formats

Overall, in contrast to initial predictions, many of the participants saw a varied difference between the file formatted images, predominantly referring to how, "The shape of her

face is different" (Lena) and the "Sharper image quality" between the file formatted images.

JPEG Vs GIF.

Several participants believed that Lena's face on the JPEG image was "thinner" and "sharper" than the GIF image. Furthermore, the "lighting" on her "right shoulder" was "different" with the JPEG (at a "higher brightness") than the GIF (at a "lower brightness") (Figure 22).



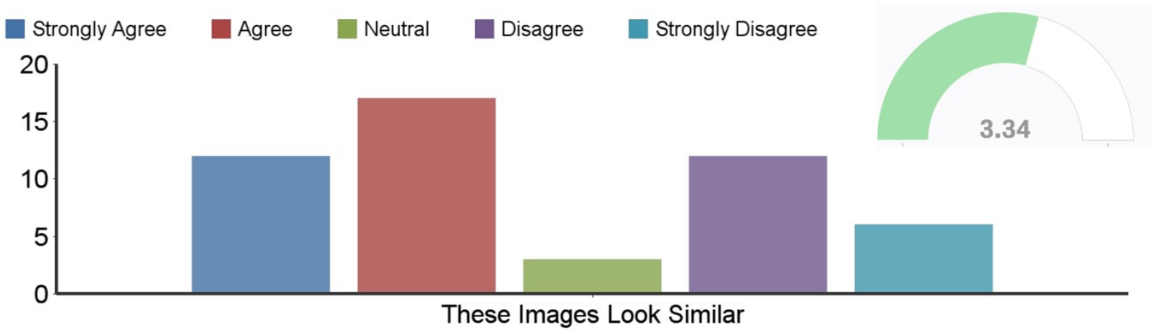
#	Question	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Response	Average Value
1	These Images Look Similar	17	16	3	9	5	50	3.62

Figure 22 - Results of JPEG Vs GIF (Lena)

The mean, shown in Figure 22 above, indicates that a JPEG and GIF file format of the same image do not share either a strong or weak similarity with a score of 3.62.

JPEG Vs PNG.

Participants claimed the content of this Lena image set was "identical" but the JPEG image still looked "sharper" than the GIF image, one participant defining the PNG as "blurry".



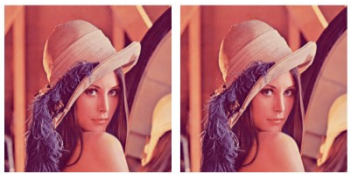
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	12	17	3	12	6	50	3.34

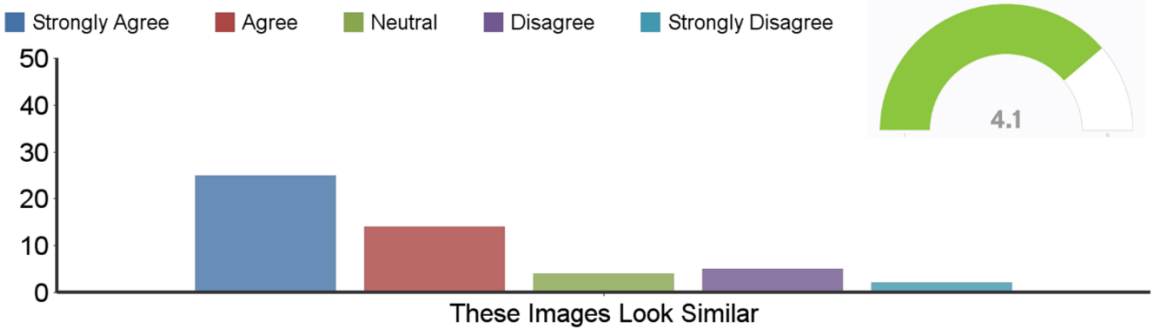
Figure 23 - Results of JPEG Vs PNG (Lena)

An average value score of 3.34 was produced by the 50 participants indicating only an average similarity between JPEG and PNG.

GIF Vs PNG.

By the third image set of file formats, many participants "could not distinguish the difference" between the Lena GIF and PNG images.





#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	25	14	4	5	2	50	4.10

Figure 24 - Results of GIF Vs PNG (Lena)

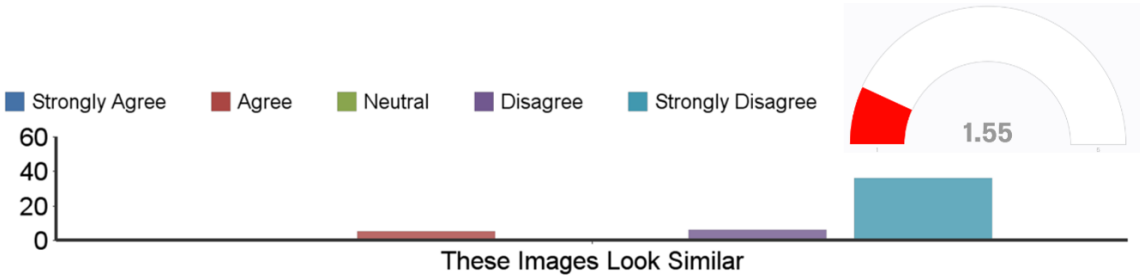
This resulted in a strong mean score of 4.10 out of the 50 respondents of the study, labelling the similarity between these two file formats as very strong.

Bit Depth

The 'Mona Lisa' image was used here and participants expressed good knowledge of this painting and could spot changes quite easily due to their previous recognition and familiarity of it. However, the human eye sees red, green and blue in different brightness levels and as this painting possesses a darker green background with no high contrast colours [62], some participants claimed that brightness and colour changes were harder to see in this painting.

24 Bit Vs 4 Bit.

Participants described the image set as "very different" visually, yet most participants still acknowledged that the manipulated image was the Mona Lisa. Participants also noticed "a severe change in colour" with the 4 bit image (which only contains a maximum of 16 available colours).



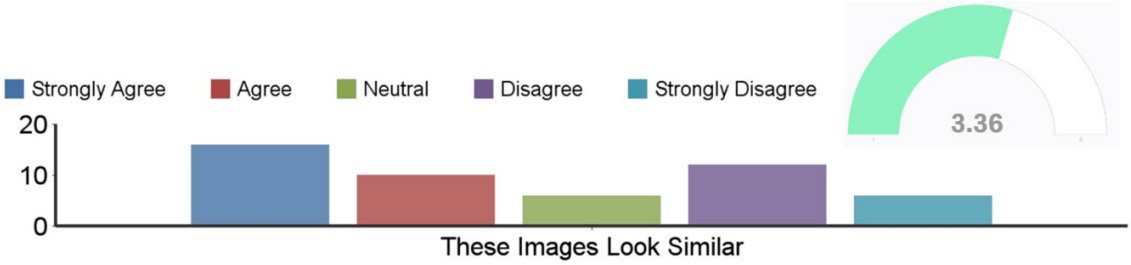
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	5	1	6	36	49	1.55

Figure 25 - Results of 24 Bit Vs 4 Bit (Mona Lisa)

The lack of colours resulted in a significant amount of 'strongly disagrees', giving a low score for this manipulated image.

8 Bit Vs 24 Bit.

Participants claimed that there was “no significant difference” between the 8 and 24 bit images, backing up claims made by other research done in this area that there is little visual difference between an 8 and 24 bit image [41]. However, a small portion of participants noticed that the sky in the background was “darker” in the 8 bit image and “lighter” in the 24 bit image.



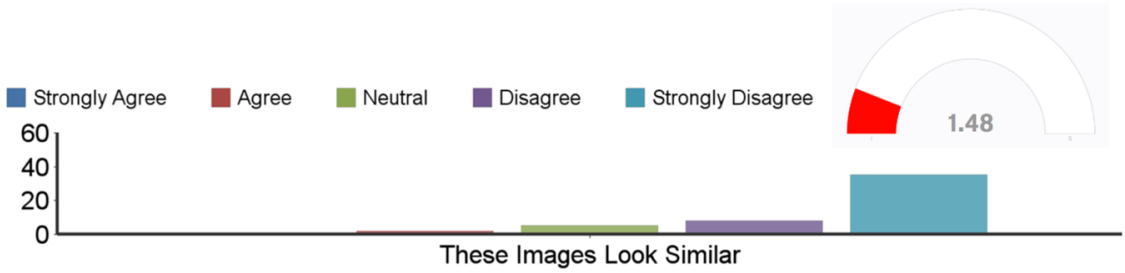
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	16	10	6	12	6	50	3.36

Figure 26 - Results of 8 Bit Vs 24 Bit (Mona Lisa)

The participants that noticed the colour changes assigned a lower score to the 8 bit image while those who did not, assigned a higher score, resulting in a 3.36 mean score value.

1 Bit Vs 24 Bit.

These images were “very different” and mainly received a strongly disagree selection, especially as the 1 bit was a greyscale image with only black and white available as colours.



#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	-	2	5	8	35	50	1.48

Figure 27 - Results of 1 Bit Vs 24 Bit (Mona Lisa)

This caused respondents to assign a low score to the similarity rating, resulting in a mean score of only 1.48. The higher scores of 2 and 3 are attributable to participants recognising the images as still being the authentic Mona Lisa.

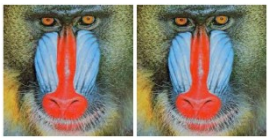
From the above the strongest steganographic technique was the 8bit Mona Lisa.

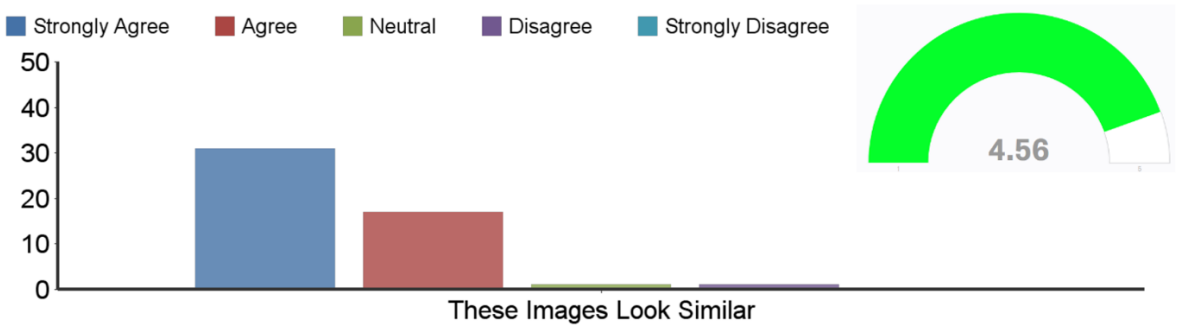
LSB Images

Although popularly used in image steganography, the Baboon image was predominantly unrecognised by participants. Generally, participants were attracted to the Baboon's eyes and the colour of the nose and cheeks when attempting to detect changes from any embedded files. One participant even focused predominantly on the yellow and orange in the fur to see if the contrast/brightness changed.

LSB 3 Vs Original.

These images were described as "very similar" where it was "very hard to distinguish the difference".





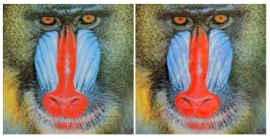
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	31	17	1	1	-	50	4.56

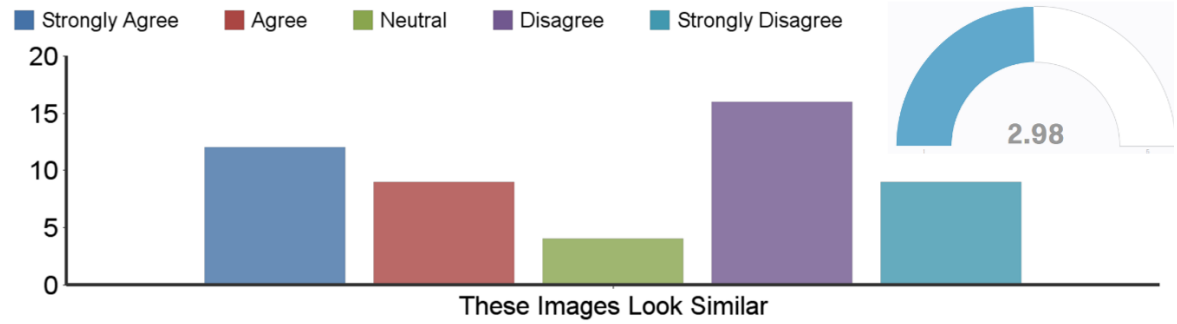
Figure 28 - LSB 3 Vs Original (Baboon)

As a result, the LSB 3 manipulated image received a very high score from respondents with no 'strongly disagree' answers given by any participant.

Original Vs LSB 5

Participants established the manipulated image was "still a baboon" but not identical to the original image. Furthermore, the manipulated image was said to be "slightly darker".





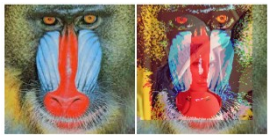
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	12	9	4	16	9	50	2.98

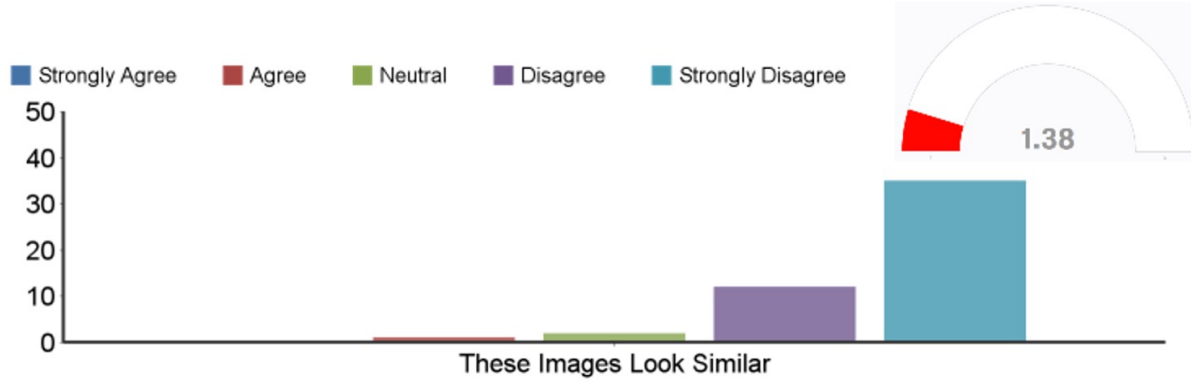
Figure 29 - Results of Original Vs LSB 5 (Baboon)

This provided an overall mean score of 2.98, neither a significantly strong or weak steganographic technique.

Original Vs LSB 7.

This image set was described as “not similar at all” due to the LSB 7 image where a “woman was clearly inside” the image. However, many respondents did acknowledge that the manipulated image was “still the baboon image”.





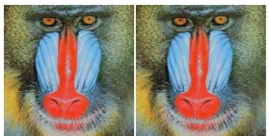
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	-	1	2	12	35	50	1.38

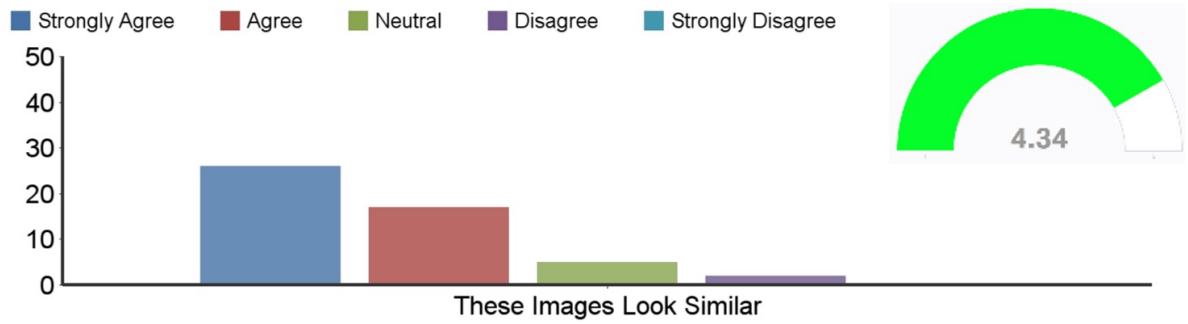
Figure 30 - Original Vs LSB 7 (Baboon)

This produced a low score of 1.38 due to the large number of respondents that noticed Lena in the Baboon cover image.

Original Vs LSB 1

Participants often spotted no difference here at all as LSB 1 manipulates very little in an image.





#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	26	17	5	2	-	50	4.34

Figure 31 - Results of Original Vs LSB 1 (Baboon)

This caused respondents to score the LSB 1 image highly with a total mean score of 4.34.

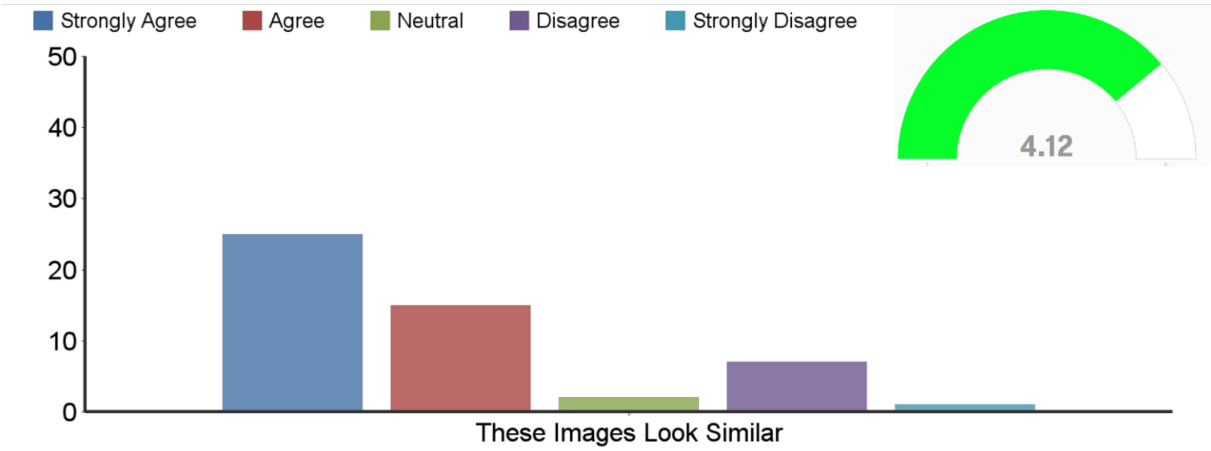
From the above work, the strongest steganographic technique was considered to be LSB3 on the Baboon image.

LSB Textual Insertion

The Union Jack was unanimously known by every participant of the study where many participants recognised the “colour changes” across the Union Jack image sets that were made with the LSB algorithm. Many participants took extra time with this section and began to doubt their perception, as some of the image sets were so alike it became difficult to establish the difference between the two images. Participants often changed their answers with even two participants asking if there were some fault with the screen of the MacBook Pro.

Original Vs 200,000 Characters LSB 1.

This image set looks “identical” and “very similar” to the original for most participants.



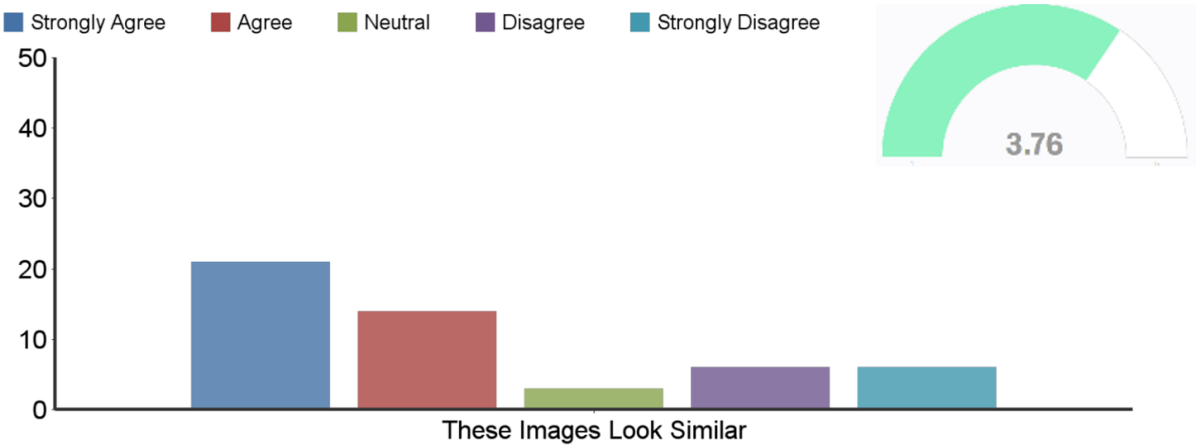
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	25	15	2	7	1	50	4.12

Figure 32 - Results of Original Vs 200,000 Characters LSB 1

An average mean score of 4.12 conveys that 200,000 characters hidden through LSB 1 is a very strong steganographic technique.

200 Characters LSB 1 Vs Original.

The second set of Union Jacks often confused participants due to their almost identical similarity to the first image set. This caused people to adjust their answers based on suspicion rather than their eyes.



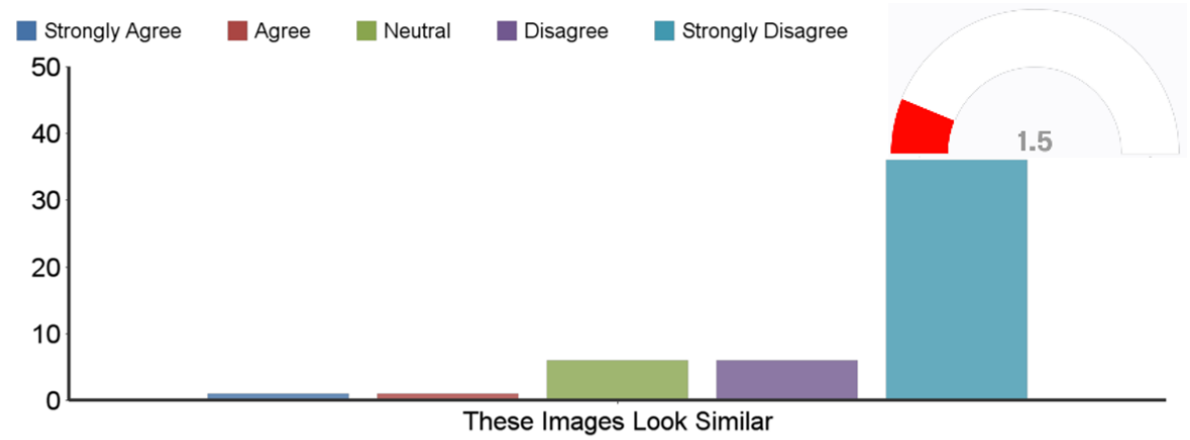
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	21	14	3	6	6	50	3.76

Figure 33 - Results of 200 Characters LSB 1 Vs Original

However, this did still score reasonably well even though there is not enough manipulation with LSB 1 to notice any significant difference visually. The doubt of human perception, especially with these images is an intriguing research area that is discussed in, *'LSB Textual Insertion – The Union Jack'*.

Original Vs 1 Million Characters LSB 8.

The manipulated image here was described as "completely different".



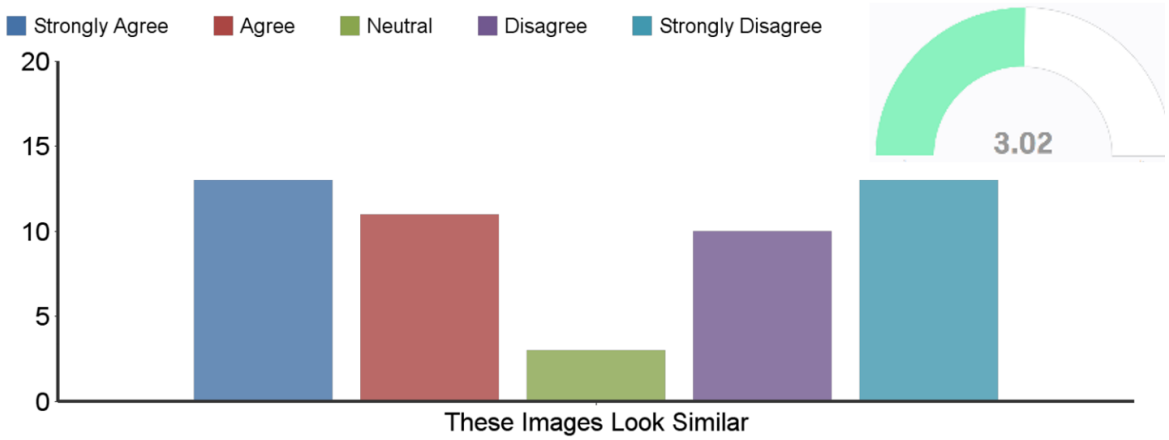
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	1	6	6	36	50	1.50

Figure 34 - Results of Original Vs 1 Million Characters LSB 8

With LSB 8 manipulation, around 40% of the image is completely disfigured with pixilation causing an expected low score of 1.50.

800,000 Characters LSB 4 Vs Original.

Some participants stated the colour was “off on one side” and one of the Union Jacks in the image set was “slightly darker in one half” of the image.



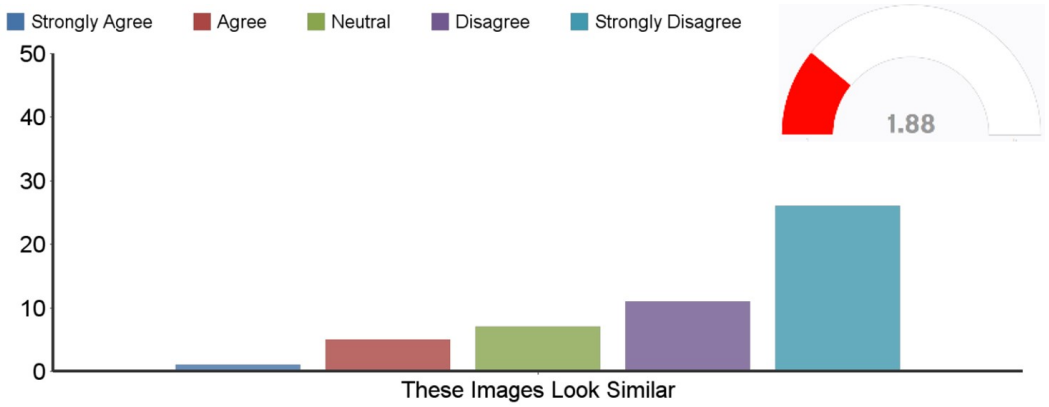
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	13	11	3	10	13	50	3.02

Figure 35 - Results of 800,000 Characters LSB 4 Vs Original

The darker side was not significant enough for the larger number of respondents to provide a lower score and the image set was given an overall score of 3.02.

Original Vs 1 Million Characters LSB 6.

Most of the participants who noticed the darker half of one of the Union Jacks in the previous image set noticed the same fault with the image but this time it was “even darker than before”.



#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	5	7	11	26	50	1.88

Figure 36 - Results of Original Vs 1 Million Characters LSB 6

As this half was “significantly darker”, this caused respondents to select a far lower score than the previous image set.

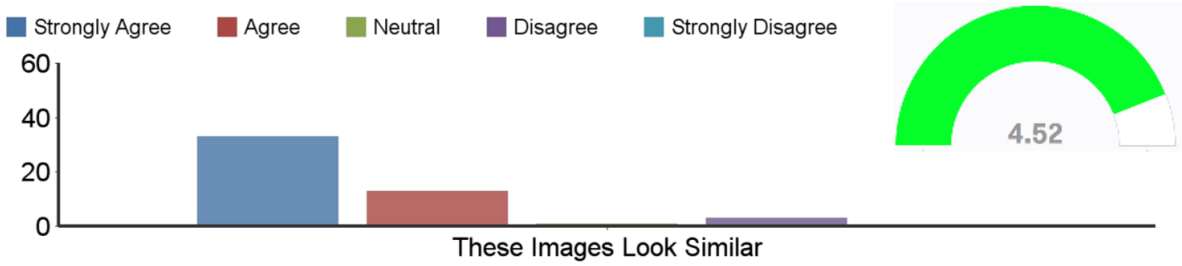
From this section of the research, the strongest steganographic technique was 200,000 characters under LSB1 with the Union Jack image.

Audio Insertion

The Scream painting was only known to a small number of participants. The painting itself contains many dim colours with low contrast of pixels, making any alterations, like the ‘The Mona Lisa’, difficult to see.

Original Vs Original with Bell (672KB).

The manipulated image seemed “brighter” but still “very similar”. Many participants claimed the two images were still “exactly the same”.



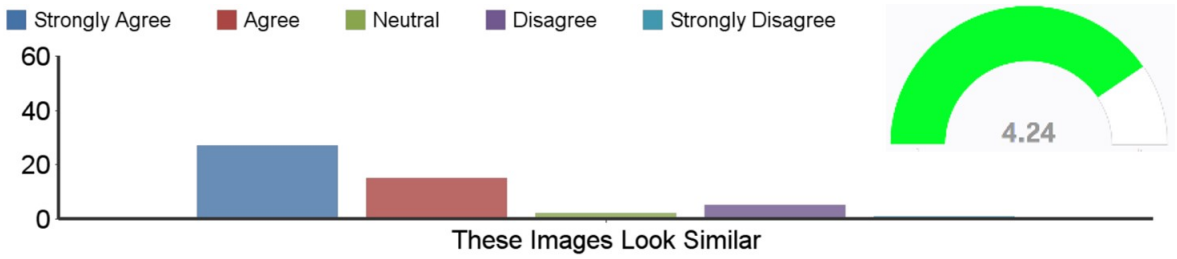
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	33	13	1	3	-	50	4.52

Figure 37 - Results of Original Vs Original w/ Bell (672KB)

The similarity of The Scream images caused many respondents to give either a 'strongly agree' or 'agree' selection with absoultely no 'stongly disagree's from any of the respondents.

Original with Ride of the Valkyries (4.57MB) Vs Original

Participants still consider this image set to be "identical".



#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	27	15	2	5	1	50	4.24

Figure 38 - Results of Original w/ Ride of the Valkyries (4.57MB) Vs Original

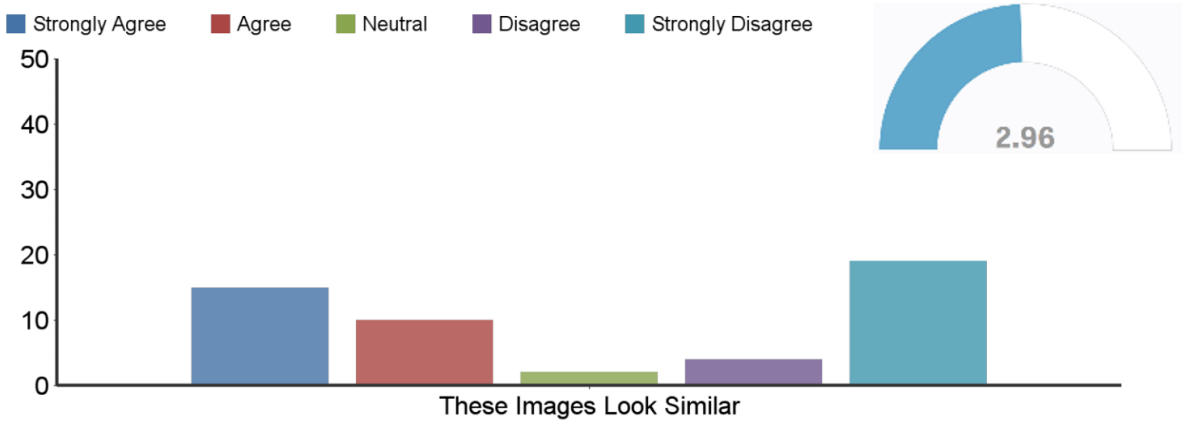
The mean score is still very high, indicating this method is very strong for visual deception.The strongest steganographic technique/conversion for this area was the original Scream image embedded with the Bell sound file (672KB).

Watermarking & Filtering

Of the 50 participants of the study, only 26 noticed the "Can You See This Message" watermark. If the participant did not spot it at first, they were then verbally asked by a supervisor, *"Are you sure you cannot see anything hidden in either of the images?".*

Original Vs Watermark with No Filter.

Participants, especially in the first image set, often looked at the objects of The Last Supper including Jesus and his disciples with some participants even counting to ensure each of the 12 disciples were in both of the images and none had been removed or duplicated. 26 participants of a total of 50 noticed the hidden message on the table cloth which caused many of these 26 to automatically select a low score.



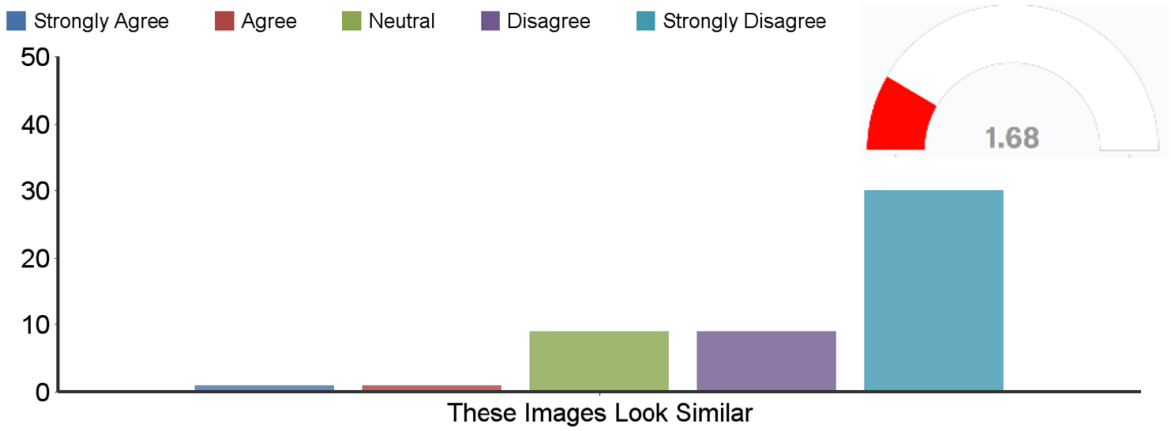
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	15	10	2	4	19	50	2.96

Figure 39 - Results of Original Vs Watermark with No Filter

Other participants who did not notice the message "could not spot any difference" in the image set and moved toward 'agree' and 'strongly agree'.

Watermark with Soften Filter Vs Original.

Respondents described the manipulated 'Soften filter' as "out of focus" and "fuzzy". The remaining respondents who already detected the hidden message in the last image set often chose 'strongly disagree' by default.



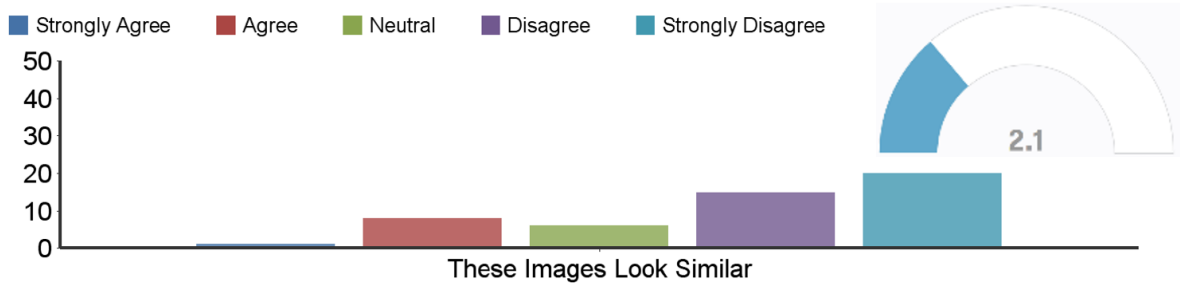
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	1	9	9	30	50	1.68

Figure 40 - Results of Watermark with Soften Filter Vs Original

The combination of the detection of the hidden message and the blurry painting caused a high number of 'strongly disagree''s to be selected.

Original Vs Watermark with Bokeh Filter.

This proved to be the best filtering technique as some participants took into consideration that this particular filter concealed the hidden text more effectively all while maintaining the original integrity of The Last Supper painting.



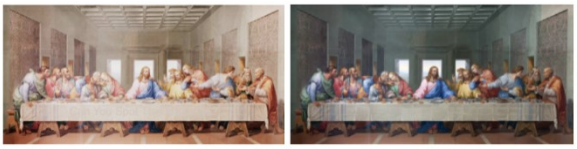
#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	8	6	15	20	50	2.10

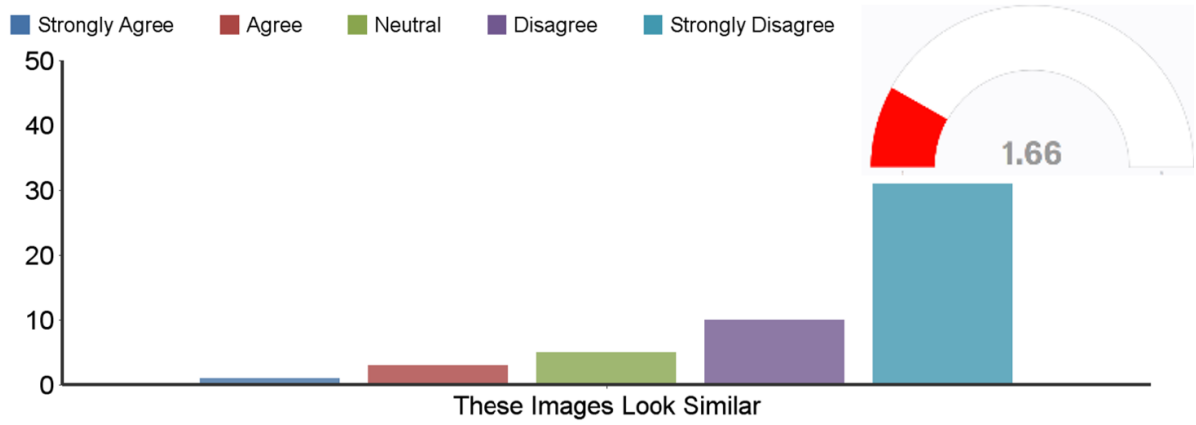
Figure 41 - Results of Original Vs Watermark with Bokeh Filter

Ones that did not take this into consideration often chose 'Strongly Disagree' by default yet again.

Watermark with Cinemara Filter Vs Original.

The manipulated image with the 'Cinemara' filter was "extremely bright" according to respondents and "looked nothing like The Last Supper".





#	Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response	Average Value
1	These Images Look Similar	1	3	5	10	31	50	1.66

Figure 42 - Results of Watermark with Cinemara Filter Vs Original

Even those that still did not spot the hidden message selected a lower score option, as the image was "completely different". Participants tended to factor in both the image alterations and the hidden message as two entirely separate modifications, resulting in a greater lean towards a lower average value score.

The strongest steganographic technique/conversion for watermarking was the **Original with No Filter.**

Experiment Duration Timings

The average time spent on the study was 5 minutes exactly. Many of the respondents started the experiment at a slower rate while their attention span was very high. The average time spent on each question then peaked toward the middle (Union Jack images) then sped up towards the end of the study (toward The Last Supper images). The faster time spent on each question toward the end could have been due to 'experiment experience' where the participant is accustomed to what is required of them during the experimentation process, enhancing their ability to make cognitive decisions quicker.

Discussion

This section provides a critical analysis of the results and processes produced by this experiment. This includes aspects of: the experimentation process; the order in which the image sets were placed; unexpected results; and decisions made by participants that may have been based on doubt rather than perception.

Critical Analysis of Results & Potential Future Work

This section will detail how each aspect tested contributes to the research field of steganography and suggests future work where necessary.

File Format – Lena

Due to the way in which this question was presented, the 'strongest' file format cannot be derived. The comparison of the file formats was included only to see if the human eye noticed a difference between file formats. Previous studies have indicated that there is a difference on a computational level [10] [28][63] with only one other study indicating that there is a difference on a visual level [18]. This work has produced results strongly indicating various visual differences in brightness, image sharpness and shapes of objects within the image.

Bit Depth – Mona Lisa

The results show that of the images tested, the 8 bit depth image of Mona Lisa was the closest, visually, to where human perception could not see a difference compared to the original. However, the 8 bit depth image, although visually similar to the original, did not have an exceptionally high mean score, indicating that it is not strong enough to be used in place of a 24 bit image. It would be fair to argue that a 12 or 16 bit image would be close enough to deceive the human eye into thinking a 12 or 16 bit depth image was the original 24 bit standard. This could be tested in future work.

LSB Images – Baboon

The LSB 3 image had the highest score based on participants' results, even higher than LSB 1 by a margin of 0.22 on the mean score. The LSB 3 image may have placed higher due to the ordering in which the image sets were placed in the Qualtrics tool. Participants may assume that the first few image sets of each steganographic/ conversion technique are "warm up sets" before the real image manipulation commences in the later image sets. Regardless, participants did have the opportunity to return to previous questions and change their answer accordingly, therefore, based on the results of this study, LSB 3 is the strongest for hiding images.

LSB Textual Insertion – The Union Jack

The first two image sets of Union Jacks were the only real anomaly when the results were produced. This was when the LSB technique that concealed 200,000 characters of text was considered to be superior in hiding information compared to only 200 characters of textual information with the exact same LSB1 placement. A strong argument could be made that the number of bits used in LSB (e.g. LSB 1, LSB2 etc.) is more important in concealing information than the amount of text that is input into the image, as documents could be split between files.

Further analysis could point toward the doubts participants were having halfway through the experiment. As the Union Jack image sets were visually very similar to each other, participants were vocal and requested the opportunity to return to a previous answer and change it. Although this was allowed during the experiment, the participant was verbally informed at the beginning of the study to *"… not let previous answers influence their current decisions".* This verbal statement did, however, seem to be disregarded due to many participants questioning and doubting their own decision making.

Audio Insertion – The Scream

The Audio insertion technique was, based on the results and mean scores, the highest scoring steganographic technique tested for the entire project. The advantage of this technique is its invisibility to the human eye if any modifications have been made to an image. The disadvantage is the high probability in which a Data Loss Prevention algorithm would detect this kind of audio insertion technique based on the very foundations of steganalysis where an image would be flagged if it contained such a large file size [61].

Furthermore, although the identities of participants cannot be disclosed in accordance with ethics, it is interesting to note that a mother and her son (both above the age of 18) taking the experiment independently, both identified a 'change in direction' of the bridge within *The Scream* image and were the only two to do so. This could perhaps indicate that perceptions of images are somewhat hereditary. This is an intriguing field for future research.

The audio input conversions also restricted the extent of the project as the Qualtrics survey software could not take any files above 16MB. Future work could include a study that analyses if humans perceive any visual changes to an image that conceal larger audio files by utilising an alternative platform to Qualtrics. In addition, the technique of copying files into other files does not efficiently conceal 'hidden information'. Both of the individual files (the audio and the

image) are simply 'added on top of one another' instead of 'blended together'. Future work should seek more efficient methods when hiding audio files in cover image files.

Watermarking & Filtering – The Last Supper

The watermark with no filter was the strongest image of 'The Last Supper' image sets, based on the mean score. Although a small amount of participants would take into consideration how effectively a filter may cover the watermarked image, most participants by default selected 'Strongly Disagree' after spotting the "Can You See This Message". However, of the filters that attempted to conceal the watermark further, the 'Bokeh' filter taken from the online image editing platform proved to be the strongest in concealing the hidden watermark message [27].

The 'Strongest' Steganography Image

The following combination of steganographic techniques included into one image would prove to be the most efficient in hiding data from the human eye, all while maintaining a low file size to go undetected by steganalysis algorithms. All recommendations are based on the results of this experimental work.

The 'Strongest' steganographic image would be:

- File Format: PNG (due to lossless compression)
    - GIF has not been selected as participants often claimed JPEG and PNG were "sharper" than GIF. JPEG was not been selected due to its lossy compression.
- 12 Bit Depth
    - This project has shown that an 8 bit depth value is close but not visually identical to a 24 bit image. Moving from 256 colours to 4096 colours (2^8 = 256, 2^12 = 4096) should replicate the 24 bit image enough to successfully go unnoticed by human perception.
- LSB 3 (for image hiding)
    - This is dependent on the cover image and the image to be hidden, yet this has proven to be the strongest of the image sets.
- LSB 1 (for textual insertion)
    - A maximum of 200,000 characters of text can be secreted successfully within an image with little visual difference to the image.
    - Note: more characters cannot be added without moving up to LSB 2.
- Less than 1MB file (for Audio insertion)
    - If the file size is too large, steganalysis algorithms will pick this up

- Ideally the vocal message should be kept short to avoid detection. If the audio message is too large, the audio file should be divided and placed within several cover images independently.

- No filter (for watermark insertion)
    - Ensure the font and colour chosen for the watermark can reflect the colour of the background of the cover image for easier blending.

Below is a table that categorises, in order of strongest to weakest, all the steganographic techniques tested in this study. Again, this excludes file formats due to the inability to categorise them in order:

Image Sets	Strongest Technique
LSB 3 Image	4.56
Original w/ Bell (672KB)	4.52
LSB 1 Image	4.34
Original w/ Ride of the Valkyries (4.57MB)	4.24
LSB 1 Text 200,000 Characters	4.12
LSB 1 Text 200 Characters	3.76
8 Bit Depth	3.36
LSB 4 800,000 Characters	3.02
LSB 5 Image	2.98
Watermark w/ No Filter	2.96
Watermark w/ Bokeh Filter	2.10
LSB 8 1 Million Characters	1.88
LSB 6 1 Million Characters	1.88
Watermark w/ Soften Filter	1.88
Watermark w/ Cinemara Filer	1.66
4 Bit Depth	1.55

1 Bit Depth	1.48
LSB 7 Image	1.38

Table 3 - Each Image Set Ranked from Strongest to Weakest

Each aspect used (i.e. File Formats, Bit Depth, LSB Images etc.) each have their image set score collected and averaged to find the mean score, providing a strength score for the overall technique for image based steganography:

Technique	Strongest
Audio Insertion	4.38
LSB Images	3.31
LSB Textual Insertion	2.93
Watermarking & Filtering	2.15
Bit Depth	2.13

Table 4 - Steganographic/Conversion Technique Ranked Strongest to Weakest

Conclusions

This work has focused on human visual perception based steganography. This area of research elicits true insight into computer security and how sophisticated images can become when manipulated for secretive purposes. Although experience can be gained from how these techniques work, human based visual inspection of images does not scale as algorithms do. With perhaps over a trillion images circulating the Internet, there will always be new images chosen for steganography based purposes.

This work has produced key results that indicate the lowest level of quality and file size, while concealing the largest amount of data, for the most efficient steganographic image, undetectable to the human eye. By knowing what the most effective ways are to conceal

information, steps can be taken in future work to enhance Data Loss Prevention systems to restrict and prevent their use, especially in matters of national, financial and industrial security.

References

[1] L. L. . Securosis, "Understanding and Selecting a Data Loss Prevention Solution," pp. 1–26, 2010.

[2] HM Government, "Technical Report," *2015 Inf. Secur. Breaches Surv.*, p. 49, 2015.

[3] BrandWatch, https://www.brandwatch.com/blog/96-amazing-social-media-statistics-and-facts/, 2018, accessed June 8 2018.

[4] CSo: IDG Contributor network: https://www.csoonline.com/article/3249088/data-breach/the-cost-of-2017-data-breaches.html, accessed June 8 2018

[5] CSo: IDG Contributor network: https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html, accessed June 8 2018

[6] Intel Security, "Data exfiltration study: Actors, tactics, and detection," *Gd. Th. Data*, pp. 30–40, 2015.

[7] D. Kahn, "The history of steganography," in *Information Hiding: First International Workshop Cambridge, U.K., May 30 -- June 1, 1996 Proceedings*, R. Anderson, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 1–5.

[8] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, 1998.

[9] B. Pfitzmann, "Information Hiding Terminology - Results of an Informal Plenary Meeting and Additional Proposals," in *Proceedings of the First International Workshop on Information Hiding*, 1996, pp. 347–350.

[10] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Comput.*, vol. 31, no. 2, pp. 26–34, 1998.

[11] W. Luo, H. Fangjun, and H. Jiwu, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *Inf. Forensics Secur. IEEE Trans.*, vol. 5, no. 2, pp. 201–214, 2010.

[12] R. M. T. Sheth, Ravi K, "Image Steganography Techniques," *Int. J. Comput. Eng. Sci.*, vol. 1, no. 2, pp. 10–15, 2015.

[13] S. Singh and A. Singh, "A Review on the Various Recent Steganography Techniques," *Int. J. Comput. Sci. Netw.*, vol. 2, no. 6, pp. 142–156, 2013.

[14] Identity Finder, "Data Loss Prevention: Data-at-Rest vs. Data-in-Motion," pp. 1–5, 2009.

[15] J. Collins and S. Agaian, "Trends toward real-time network data steganography," pp. 1–20, 2016.

[16] Ernst & Young, "Data Loss Prevention - Keeping your sensitive data out of the public

domain," *Insights governance, risk compliance*, no. October, 2011.

[17] G. Berg, I. Davidson, M.-Y. Duan, and G. Paul, "Searching for Hidden Messages: Automatic Detection of Steganography.," *Am. Assoc. Artif. Intell.*, pp. 51–56, 2003.

[18] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An Overview of Image Steganography," *Inf. Comput. Secur. Archit. Res. Gr.*, vol. 83, no. July, pp. 51–107, 2005.

[19] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," *IEEE Conf. Mil. Commun.*, pp. 216–220, 1990.

[20] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, 1997.

[21] K. Choudhary, "Image Steganography and Global Terrorism," *Glob. Secur. Stud.*, vol. 3, no. 4, pp. 34–48, 2012.

[22] T. Kellen, "Hiding in Plain View: Could Steganography be a terrorist tool," *SANS Inst. InfoSec Read. Room*, pp. 1–8, 2001.

[23] M. Hart, P. Manadhata, and R. Johnson, *Text Classification for Data Loss Prevention*. 2011.

[24] A. Kumar and R. Sharma, "International Journal of Advanced Research in A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 7, pp. 363–372, 2013.

[25] R. Popa, "An Analysis of Steganographic Techniques," pp. 7–8, 1998.

[26] R. P. Jonathon Cummins, Patrick Diskin, Samuel Lau, "Steganography And Digital Watermarking," pp. 1–24, 2004.

[27] Pic Monkey, "Photo Editor," 2016. [Online]. Available: https://www.picmonkey.com/photo-editor. [Accessed: 26-Jul-2016].

[28] L. McGill, "Steganography: The Right Way," *SANS Inst. InfoSec Read. Room*, p. 18, 2005.

[29] Data Genetics, "Steganography," 2012. [Online]. Available: http://datagenetics.com/blog/march12012/index.html.

[30] S. Venkatraman, A. Abraham, and M. Paprzycki, "Significance of steganography on data security," in *International Conference on Information Technology: Coding Computing, ITCC*, 2004, vol. 2, pp. 347–351.

[31] ISO/IEC, "Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification," 2004.

[32] L. Zhi, S. A. Fen, and Y. Y. Xian, "A LSB steganography detection algorithm," in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, 2003, vol. 3, pp. 2780–2783.

[33] C. Manikopoulos, Y.-Q. Shi, S. Song, Z. Zhang, Z. Ni, and D. Zou, "Detection of block DCT-based steganography in gray-scale images," in *Multimedia Signal Processing, 2002 IEEE Workshop on*, 2002, pp. 355–358.

[34] C. Zhi-li, H. Liu-sheng, Y. Zhen-shan, L. Ling-jun, and Y. Wei, “A statistical algorithm for linguistic steganography detection based on distribution of words,” in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, 2008, pp. 558–563.

[35] J. Fridrich, M. Goljan, and R. Du, “Reliable Detection of LSB Steganography in Grayscale and Color Images,” *Proc. ACM Work. Multimed. Secur.*, pp. 27–30, 2001.

[36] J. T. Townsend, “Serial Vs Parallel Processing : Sometimes They Look Like Tweedledum and Tweedledee but They Can (and Should) be Distinguished,” *Psychol. Sci.*, vol. 1, no. 1, pp. 46–54, 1990.

[37] S. Parah, J. Sheikh, J. . Akhoon, and G. Bhat, “High Capacity Data Hiding using Random Plane Indicator Technique for color images High Capacity Data Hiding using Random Plane Indicator Technique for color images,” *2015 Int. Conf. Adv. Comput. Commun. Electron. Eng.*, no. April 2016, 2015.

[38] V. K. Mann and H. S. Dhaliwal, “32 × 32 Colour Image Steganography,” *Int. J. Eng. Trends Technol.*, vol. 4, no. 8, pp. 3687–3690, 2013.

[39] Hexed, “Hex Editor,” 2016. [Online]. Available: https://hexed.it/. [Accessed: 18-Aug-2016].

[40] P. Meerwald, “Lena RGB Color,” 2016. .

[41] Bluebeam, “Reduced File Size,” pp. 1–13, 2007.

[42] M. Lisa, T. B. Girl, W. Wide, W. Author, and D. S. Source, “Mona Lisa : the Best-Known Girl in the Whole Wide World * by Donald Sassoon,” vol. 51, no. 51, pp. 1–18, 2015.

[43] L. Da Vinci, “Mona Lisa Painting,” 1506. [Online]. Available: https://upload.wikimedia.org/wikipedia/commons/thumb/e/ec/Mona_Lisa,_by_Leonardo_da_Vinci,_from_C2RMF_retouched.jpg/687px-Mona_Lisa,_by_Leonardo_da_Vinci,_from_C2RMF_retouched.jpg. [Accessed: 16-Jul-2016].

[44] L. Stanwood, “Specifying Color,” *Constr. Specif.*, 1983.

[45] GIMP, “Change The Mode,” *Gimp Online Documentation*, 2014. .

[46] G. A. Y. Steven J. Friedman, Karen A. Hargrove, Joseph M. Joy, Nathan P. Myhrvold, Sunita Shrivastava, “Method and apparatus for mapping colors in an image through dithering and diffusion,” *US Patents*, 1995.

[47] J. Stanley, “Incoherency,” 2016. [Online]. Available: http://incoherency.co.uk/image-steganography/. [Accessed: 10-Jul-2016].

[48] ManyTools, “Steganography (encode text into image),” 2013. [Online]. Available: http://manytools.org/hacker-tools/steganography-encode-text-into-image/. [Accessed: 20-Jul-2016].

[49] Y. Wang, “StegoUI,” 2016. [Online]. Available: https://github.com/YunjiaGH/stegoUI.

[50] Y. Wang, “An Effective Solution for DLP Systems: Preventing Message Loss Through Inside Steganography,” St-Andrews, 2016.

[51] TextMechanic, “Random String Generator,” 2016. [Online]. Available: http://textmechanic.com/text-tools/randomization-tools/random-string-generator/. [Accessed: 24-Jul-2016].

[52] SoundJay, “Bell Sound Effects,” 2016. [Online]. Available: http://www.soundjay.com/bell-sound-effect.html. [Accessed: 22-Jul-2016].

[53] J.-S. Pan, *Intelligent multimedia data hiding new directions*, vol. 58. Springer, 2007.

[54] ArtExperts, “Edvard Munch (1863-1944),” 2016. [Online]. Available: https://www.artexpertswebsite.com/pages/artists/munch.php. [Accessed: 23-Jul-2016].

[55] Instructables, “MP3-GIF: Hide Music Inside A Picture,” 2015. [Online]. Available: http://www.instructables.com/id/MP3-GIF%3A-Hide-Music-Inside-A-Picture/step4/Combining-the-MP3-and-the-GIF/. [Accessed: 24-Jul-2016].

[56] YouTube, “Richard Wagner - Ride Of The Valkyries,” 2008. [Online]. Available: https://www.youtube.com/watch?v=GGU1P6lBW6Q. [Accessed: 24-Jul-2016].

[57] YouTubeMP3, “YouTube to MP3 Converter.” [Online]. Available: http://www.youtube-mp3.org/. [Accessed: 24-Jul-2016].

[58] U.-D. Reips, “The web experiment: advantages, disadvantages, and solutions,” *Psychol. Exp. Internet*, pp. 89–117, 2000.

[59] Apple, “MacBook Pro User ’ s Guide MacBook Pro computer,” 2006.

[60] A. K. Ericsson, “Protocol Analysis and Expert Thought : Concurrent Verbalizations of Thinking during Experts ’ Performance on Representative Tasks,” in *The Cambridge Handbook of Expertise and Expert Performance*, 2006, pp. 39–68.

[61] R. Johns, “Likert Items and Scales,” vol. 1, no. March, pp. 1–11, 2010.

[62] J. Lawrence, “Human Vision, Color and Basic Image Processing,” 2011. [Online]. Available: http://www.cs.virginia.edu/~gfx/Courses/2011/IntroGraphics/lectures/2-Image.pdf.

[63] D. Santa-Cruz and T. Ebrahimi, “An analytical study of JPEG 2000 functionalities,” *Proc. 2000 Int. Conf. Image Process. (Cat. No.00CH37101)*, pp. 49–52 vol.2, 2000.

[64] K. Curran and J. M. Devitt, “Image Analysis for Online Dynamic Steganography Detection,” *Comput. Inf. Sci.*, vol. 1, no. 3, pp. 32–41, 2008.

Appendices

Experimental Tool Screenshots

These are included here for completeness but the information will be available online if accepted.

Questionnaire Information

I ...

- Have a Computer Science Background
- Do Not Have a Computer Science Background
- Would Prefer Not To Answer

My age is ...

0 10 20 30 40 50 60 70 80 90 100

Slide This Bar

I wear Glasses

- Yes
- Sometimes
- No

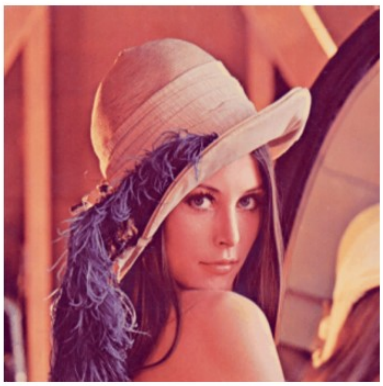
0% 100%

>>

Online Image Questionnaire

University of St Andrews

Questions - Please Take 10 Seconds Minimum to Analyse Each Question Carefully

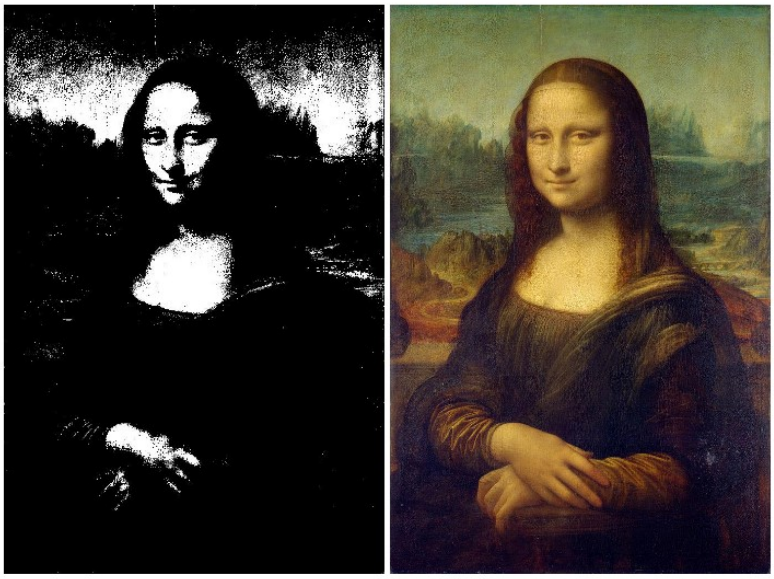
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
These Images Look Similar	○	○	○	○	○

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

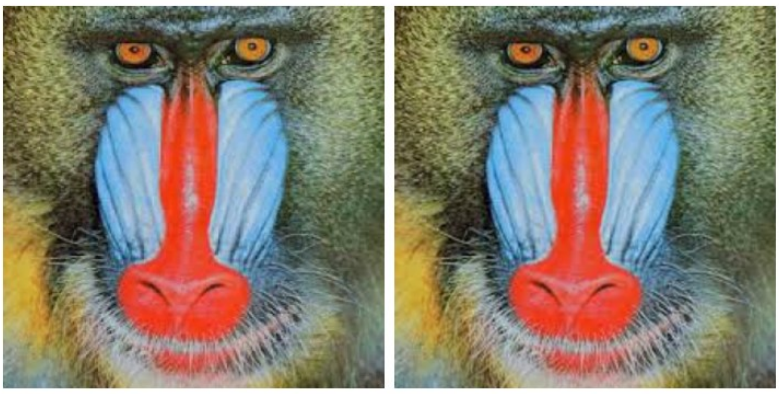
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

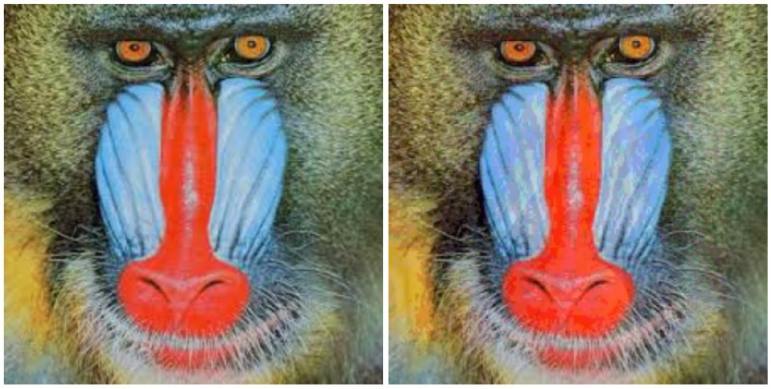
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

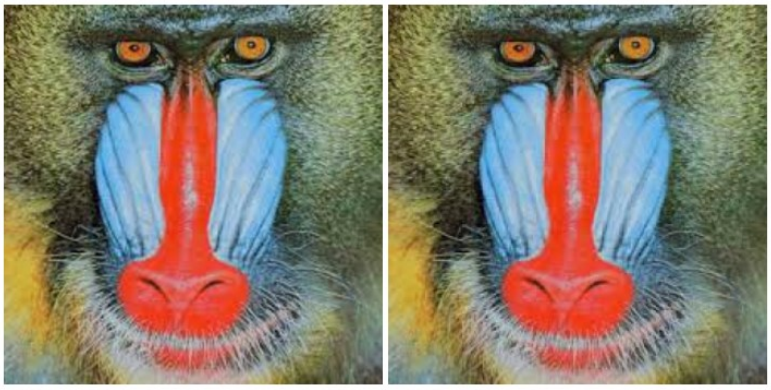


	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar					

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar					

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar					

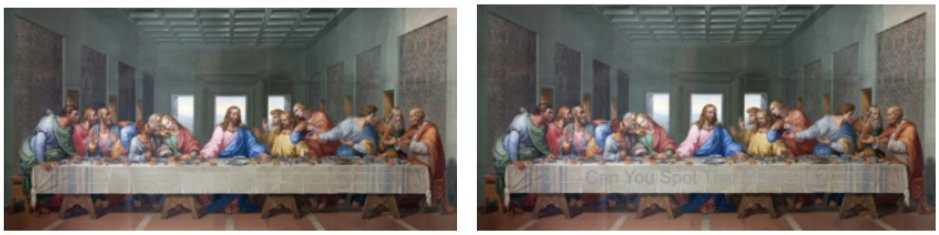
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

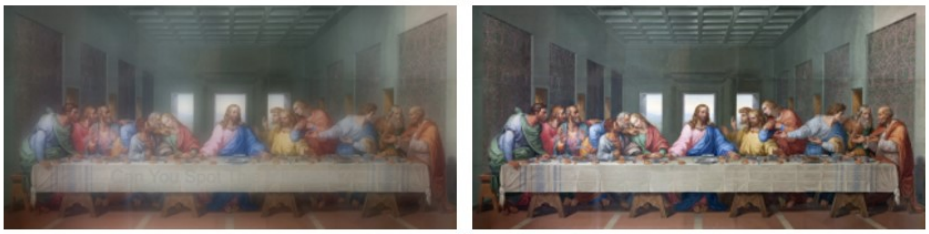
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○

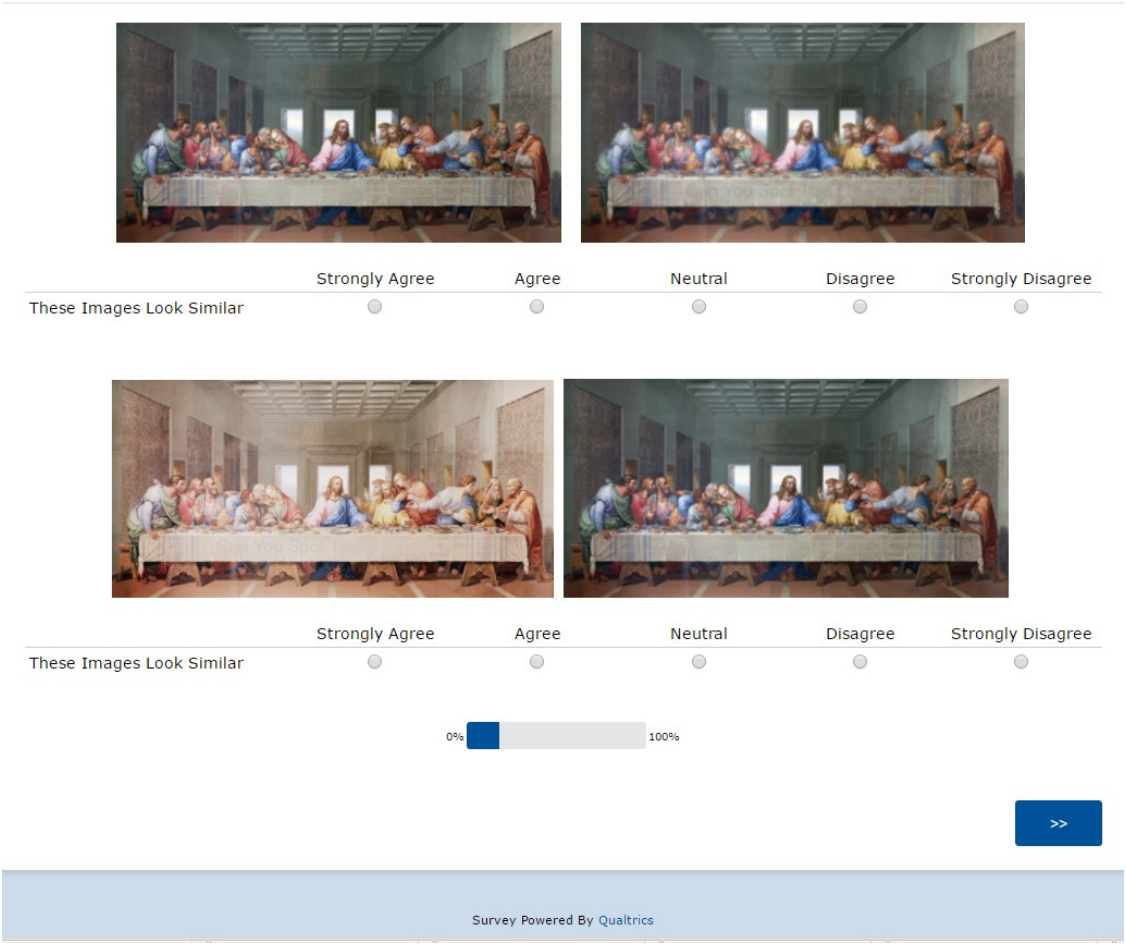
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
These Images Look Similar	○	○	○	○	○



Results

The full results are here:

https://drive.google.com/file/d/0B63fdDDLlGAJaFFwU1VabDZfaFU/view?usp=sharing

#	Scoring	Answer	Bar	Response	%
1	✓	Have a Computer Science Background		21	42.00%
2	✓	Do Not Have a Computer Science Background		29	58.00%
3	✓	Would Prefer Not To Answer		0	0.00%
		Total		50	100.00%